

03560.002936



PATENT APPLICATION

03CO

#3  
LM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: )  
: Examiner: N.Y.A.  
KOJIRO KATAYAMA ET AL. )  
: Group Art Unit: N.Y.A.  
Application No.: 09/987,487 / )  
: Filed: November 15, 2001 )  
: For: INFORMATION PROCESSING METHOD )  
FOR MANAGING EQUIPMENT, :  
EQUIPMENT MANAGING PROGRAM, )  
RECORDING MEDIUM STORING :  
EQUIPMENT MANAGING PROGRAM, )  
AND EQUIPMENT MANAGING METHOD : January 2, 2002

Commissioner for Patents  
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENT

Sir:

In support of Applicants' claim for priority under 35 U.S.C. § 119, enclosed  
is a certified copy of the following foreign application:  
2000-351262, filed November 17, 2000.

Applicants' undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

  
\_\_\_\_\_  
Attorney for Applicants

Registration No. 29,286

FITZPATRICK, CELLA, HARPER & SCINTO  
30 Rockefeller Plaza  
New York, New York 10112-3801  
Facsimile: (212) 218-2200

NY-MAIN228036v1



CFG 2936 US  
09/987,487

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年11月17日

出願番号

Application Number:

特願2000-351262

出願人

Applicant(s):

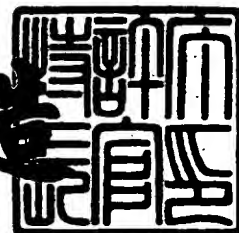
キヤノン株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年12月 7日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



【書類名】 特許願

【整理番号】 4354010

【提出日】 平成12年11月17日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G06F 1/00

【発明の名称】 情報処理装置、機器管理プログラム、機器管理プログラムが格納された記録媒体、及び機器管理方法

【請求項の数】 40

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 片山 康二郎

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 中村 真一

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 原 寛之

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 廣瀬 淳一

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 大森 和志

【発明者】

【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号キヤノン株式会社  
内

【氏名】 川島 真

【特許出願人】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号

【氏名又は名称】 キヤノン株式会社

【代表者】 御手洗 富士夫

【電話番号】 03-3758-2111

【代理人】

【識別番号】 100090538

【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号キヤノン株式会社  
内

【弁理士】

【氏名又は名称】 西山 恵三

【電話番号】 03-3758-2111

【選任した代理人】

【識別番号】 100096965

【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号キヤノン株式会  
社内

【弁理士】

【氏名又は名称】 内尾 裕一

【電話番号】 03-3758-2111

【手数料の表示】

【予納台帳番号】 011224

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9908388

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置、機器管理プログラム、機器管理プログラムが格納された記録媒体、及び機器管理方法

【特許請求の範囲】

【請求項 1】 第 1 タイプの機器とローカルネットワークを介して接続され、前記第 1 タイプの機器を管理する第 1 ローカルサーバと、第 2 タイプの機器とローカルネットワークを介して接続され、前記第 2 タイプの機器を管理する第 2 ローカルサーバと接続されている情報処理装置であって、

前記第 1 タイプの機器における障害であるか、前記第 2 タイプの機器における障害であるかを判定する判定手段と、

前記判定手段による判定結果に基づいて、前記第 1 ローカルサーバに、又は前記第 2 ローカルサーバに、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに診断を行なわせる診断制御手段とを有することを特徴とする情報処理装置。

【請求項 2】 前記診断制御手段は、前記第 1 ローカルサーバに対して、又は前記第 2 ローカルサーバに対して、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに対して、診断要求を発行することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記ローカルネットワークに接続されている機器の一覧を表示部に表示させる表示制御手段を有することを特徴とする請求項 1 或いは 2 に記載の情報処理装置。

【請求項 4】 前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定されない場合、復旧作業に向うようにサービスマンに通知する第 1 通知手段を有することを特徴とする請求項 1 乃至 3 のいずれかに記載の情報処理装置。

【請求項 5】 前記第 1 通知手段は、サービスマンが所有する携帯端末に、復旧作業に向う向かい先を示す情報を送信することを特徴とする請求項 4 に記載の情報処理装置。

【請求項 6】 前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによっ

て障害が特定される場合、障害内容を示すレポート情報を生成するレポート生成手段を有することを特徴とする請求項 1 乃至 5 のいずれかに記載の情報処理装置。

【請求項 7】 障害に対して自社が対応できない場合、復旧作業の依頼を他社に通知する第 2 通知手段を有することを特徴とする請求項 1 乃至 6 のいずれかに記載の情報処理装置。

【請求項 8】 前記第 1 タイプの機器は周辺機器であり、前記第 2 タイプの機器はコンピュータ機器であることを特徴とする請求項 1 乃至 7 のいずれかに記載の情報処理装置。

【請求項 9】 前記第 1 タイプの機器は、プリンタ、複写機、スキャナのうちの少なくとも一つであることを特徴とする請求項 8 に記載の情報処理装置。

【請求項 10】 前記第 2 タイプの機器は、パーソナルコンピュータ、サーバコンピュータ、ネットワーク機器のうちの少なくとも一つであることを特徴とする請求項 8 に記載の情報処理装置。

【請求項 11】 第 1 タイプの機器とローカルネットワークを介して接続され、前記第 1 タイプの機器を管理する第 1 ローカルサーバと、第 2 タイプの機器とローカルネットワークを介して接続され、前記第 2 タイプの機器を管理する第 2 ローカルサーバと接続されている情報処理装置で実行される機器管理プログラムであって、

前記第 1 タイプの機器における障害であるか、前記第 2 タイプの機器における障害であるかを判定する判定ステップと、

前記判定ステップによる判定結果に基づいて、前記第 1 ローカルサーバに、又は前記第 2 ローカルサーバに、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに診断を行なわせる診断制御ステップとをコンピュータに実行させることを特徴とする機器管理プログラム。

【請求項 12】 前記診断制御ステップは、前記第 1 ローカルサーバに対して、又は前記第 2 ローカルサーバに対して、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに対して、診断要求を発行することを特徴とする請求項 11 に記載の機器管理プログラム。



【請求項 13】 前記ローカルネットワークに接続されている機器の一覧を表示部に表示させる表示制御ステップをコンピュータに実行させることを特徴とする請求項 11 或いは 12 に記載の機器管理プログラム。

【請求項 14】 前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定されない場合、復旧作業に向うようにサービスマンに通知する第 1 通知ステップをコンピュータに実行させることを特徴とする請求項 11 乃至 13 のいずれかに記載の機器管理プログラム。

【請求項 15】 前記第 1 通知ステップは、サービスマンが所有する携帯端末に、復旧作業に向う向かい先を示す情報を送信することを特徴とする請求項 14 に記載の機器管理プログラム。

【請求項 16】 前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定される場合、障害内容を示すレポート情報を生成するレポート生成ステップをコンピュータに実行させることを特徴とする請求項 11 乃至 15 のいずれかに記載の機器管理プログラム。

【請求項 17】 障害に対して自社が対応できない場合、復旧作業の依頼を他社に通知する第 2 通知ステップをコンピュータに実行させることを特徴とする請求項 11 乃至 16 のいずれかに記載の機器管理プログラム。

【請求項 18】 前記第 1 タイプの機器は周辺機器であり、前記第 2 タイプの機器はコンピュータ機器であることを特徴とする請求項 11 乃至 17 のいずれかに記載の機器管理プログラム。

【請求項 19】 前記第 1 タイプの機器は、プリンタ、複写機、スキャナのうちの少なくとも一つであることを特徴とする請求項 18 に記載の機器管理プログラム。

【請求項 20】 前記第 2 タイプの機器は、パーソナルコンピュータ、サーバコンピュータ、ネットワーク機器のうちの少なくとも一つであることを特徴とする請求項 18 に記載の機器管理プログラム。

【請求項 21】 第 1 タイプの機器とローカルネットワークを介して接続され、前記第 1 タイプの機器を管理する第 1 ローカルサーバと、第 2 タイプの機器とローカルネットワークを介して接続され、前記第 2 タイプの機器を管理する第

2 ローカルサーバと接続されている情報処理装置で実行される機器管理プログラムが格納されたコンピュータにより読取り可能な記録媒体であって、前記機器管理プログラムは、

前記第 1 タイプの機器における障害であるか、前記第 2 タイプの機器における障害であるかを判定する判定ステップと、

前記判定ステップによる判定結果に基づいて、前記第 1 ローカルサーバに、又は前記第 2 ローカルサーバに、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに診断を行なわせる診断制御ステップとをコンピュータに実行させることを特徴とする記録媒体。

【請求項 2 2】 前記診断制御ステップは、前記第 1 ローカルサーバに対して、又は前記第 2 ローカルサーバに対して、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに対して、診断要求を発行することを特徴とする請求項 2 1 に記載の記録媒体。

【請求項 2 3】 前記機器管理プログラムは、前記ローカルネットワークに接続されている機器の一覧を表示部に表示させる表示制御ステップをコンピュータに実行させることを特徴とする請求項 2 1 或いは 2 2 に記載の記録媒体。

【請求項 2 4】 前記機器管理プログラムは、前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定されない場合、復旧作業に向うようにサービスマンに通知する第 1 通知ステップをコンピュータに実行させることを特徴とする請求項 2 1 乃至 2 3 のいずれかに記載の記録媒体。

【請求項 2 5】 前記第 1 通知ステップは、サービスマンが所有する携帯端末に、復旧作業に向う向かい先を示す情報を送信することを特徴とする請求項 2 4 に記載の記録媒体。

【請求項 2 6】 前記機器管理プログラムは、前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定される場合、障害内容を示すレポート情報を生成するレポート生成ステップをコンピュータに実行させることを特徴とする請求項 2 1 乃至 2 5 のいずれかに記載の記録媒体。

【請求項 2 7】 前記機器管理プログラムは、障害に対して自社が対応できない場合、復旧作業の依頼を他社に通知する第 2 通知ステップをコンピュータに

実行させることを特徴とする請求項 2 1 乃至 2 6 のいずれかに記載の記録媒体。

【請求項 2 8】 前記第 1 タイプの機器は周辺機器であり、前記第 2 タイプの機器はコンピュータ機器であることを特徴とする請求項 2 1 乃至 2 7 のいずれかに記載の記録媒体。

【請求項 2 9】 前記第 1 タイプの機器は、プリンタ、複写機、スキャナのうちの少なくとも一つであることを特徴とする請求項 2 8 に記載の記録媒体。

【請求項 3 0】 前記第 2 タイプの機器は、パーソナルコンピュータ、サーバコンピュータ、ネットワーク機器のうちの少なくとも一つであることを特徴とする請求項 2 8 に記載の記録媒体。

【請求項 3 1】 第 1 タイプの機器とローカルネットワークを介して接続され、前記第 1 タイプの機器を管理する第 1 ローカルサーバと、第 2 タイプの機器とローカルネットワークを介して接続され、前記第 2 タイプの機器を管理する第 2 ローカルサーバと、前記第 1 ローカルサーバと前記第 2 ローカルサーバとに接続されているセンタサーバから構成されるシステムで実行される機器管理方法であって、

前記第 1 タイプの機器における障害であるか、前記第 2 タイプの機器における障害であるかを判定する判定ステップと、

前記判定ステップによる判定結果に基づいて、前記第 1 ローカルサーバに、又は前記第 2 ローカルサーバに、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに診断を行なわせる診断制御ステップとを有することを特徴とする機器管理方法。

【請求項 3 2】 前記診断制御ステップは、前記第 1 ローカルサーバに対して、又は前記第 2 ローカルサーバに対して、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに対して、診断要求を発行することを特徴とする請求項 3 1 に記載の機器管理方法。

【請求項 3 3】 前記ローカルネットワークに接続されている機器の一覧を表示部に表示させる表示制御ステップを有することを特徴とする請求項 3 1 或いは 3 2 に記載の機器管理方法。

【請求項 3 4】 前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによ

って障害が特定されない場合、復旧作業に向うようにサービスマンに通知する第 1 通知ステップを有することを特徴とする請求項 3 1 乃至 3 3 のいずれかに記載の機器管理方法。

【請求項 3 5】 前記第 1 通知ステップは、サービスマンが所有する携帯端末に、復旧作業に向う向かい先を示す情報を送信することを特徴とする請求項 3 4 に記載の機器管理方法。

【請求項 3 6】 前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定される場合、障害内容を示すレポート情報を生成するレポート生成ステップを有することを特徴とする請求項 3 1 乃至 3 5 のいずれかに記載の機器管理方法。

【請求項 3 7】 障害に対して自社が対応できない場合、復旧作業の依頼を他社に通知する第 2 通知ステップを有することを特徴とする請求項 3 1 乃至 3 6 のいずれかに記載の機器管理方法。

【請求項 3 8】 前記第 1 タイプの機器は周辺機器であり、前記第 2 タイプの機器はコンピュータ機器であることを特徴とする請求項 3 1 乃至 3 7 のいずれかに記載の機器管理方法。

【請求項 3 9】 前記第 1 タイプの機器は、プリンタ、複写機、スキャナのうちの少なくとも一つであることを特徴とする請求項 3 8 に記載の機器管理方法。

【請求項 4 0】 前記第 2 タイプの機器は、パーソナルコンピュータ、サーバコンピュータ、ネットワーク機器のうちの少なくとも一つであることを特徴とする請求項 3 8 に記載の機器管理方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、たとえばコンピュータネットワークを介して接続された、汎用性のあるパーソナルコンピュータ（PC）やサーバコンピュータといった PC・サーバ系機器と、専用の機能、特にプリンタや複写機、スキャンといった入出力機能に特化した周辺機器（デバイス）系機器の状態を、包括的に遠隔監視する遠隔サ

イト管理システムに関するものである。

【0002】

【従来の技術】

従来、オフィス内の機器に関する稼動情報、エラー情報、ログ情報などをオフィス内で収集するような監視・管理システムは存在していた。また、そのようにオフィスで収集された情報をネットワークを介してオフィスの外部に設置・接続されたセンタサーバに収集し監視・管理するようなシステムも存在していた。

【0003】

しかしながら、それらの管理・監視システムはPC・サーバ系すなわち汎用コンピュータのみを監視・管理するようなシステムであったり、プリンタや複写機などのデバイス系のみを監視・管理するようなシステムであった。

【0004】

このように、汎用コンピュータとデバイスとが別個に管理されていたのは、汎用コンピュータとデバイスとを管理する手順等が全く異なるためである。すなわち、汎用コンピュータを管理する場合には、コンピュータのオペレーティングシステム等の環境に応じて所望の機能を果たすプログラムを作成し、管理対象のコンピュータで実行させることが必要であるのに対して、周辺機器を管理する場合には、機能の後付や変更が實際上ほとんど不可能であった。

【0005】

加えて、周辺機器を管理する場合、監視・管理システムが周辺機器とやりとりするデータ形式や交換の手順（プロトコル）に標準的なものが存在しなかった。そのため、周辺機器ごとに対応した管理手順を開発しなければならず、個々の周辺機器がそれぞれ管理サイトに接続され、管理されていた。

【0006】

このようにデバイス系の管理システムはPC・サーバ系の管理システムとは相容れず、それぞれ全く別個に存在していた。

【0007】

【発明が解決しようとする課題】

その一方、デバイス系の周辺機器とPC・サーバ系のコンピュータが共にオフ

イス環境で普及するにつれて、それらを統括的に監視・管理する保守サービスが望まれている。

【0008】

しかし、従来の方法では、保守サービス会社（管理サイト）が、あるオフィスのデバイス系とPC・サーバ系との両方を監視・管理するためには、両方のシステムをオフィスに設置して、別々の回線を通じて情報を収集し、別々に監視・管理しなければならなかった。そのため、保守サービス会社における管理の煩雑化、システムの運用費・維持費の高価格化が生じた。

【0009】

そこで、本発明は、上記問題点を鑑みてなされたものであり、管理サイトが、オフィスにおけるPC・サーバ系の機器とデバイス系の機器との双方を、一元的に管理できる遠隔サイト管理システムを提供することを目的とする。

【0010】

特に、オフィスのサービス対象の機器がエラーを起こし、オフィスの顧客が保守サービス会社に電話で通知（センターコール）したときに、エラー発生に的確に対応し、スムーズにメンテナンスの手配（サービスマンの手配、他のサービス会社への代行メンテナンス依頼）を行なう遠隔サイト管理システムを提供することを目的とする。

【0011】

【課題を解決するための手段】

本発明は、第1タイプの機器とローカルネットワークを介して接続され、前記第1タイプの機器を管理する第1ローカルサーバと、第2タイプの機器とローカルネットワークを介して接続され、前記第2タイプの機器を管理する第2ローカルサーバと接続されている場合であって、前記第1タイプの機器における障害であるか、前記第2タイプの機器における障害であるかを判定し、判定結果に基づいて、前記第1ローカルサーバに、又は前記第2ローカルサーバに、又は前記第1ローカルサーバと前記第2ローカルサーバとに診断を行なわせることを特徴とする。

【0012】

さらに、本発明では、前記第 1 ローカルサーバに対して、又は前記第 2 ローカルサーバに対して、又は前記第 1 ローカルサーバと前記第 2 ローカルサーバとに対して、診断要求を発行することを特徴とする。

【 0 0 1 3 】

さらに、本発明では、前記ローカルネットワークに接続されている機器の一覧を表示部に表示させる。

【 0 0 1 4 】

さらに、本発明では、前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定されない場合、復旧作業に向うようにサービスマンに通知することを特徴とする。

【 0 0 1 5 】

さらに、本発明では、サービスマンが所有する携帯端末に、復旧作業に向う向かい先を示す情報を送信することを特徴とする。

【 0 0 1 6 】

さらに、本発明では、前記第 1 ローカルサーバ又は前記第 2 ローカルサーバによって障害が特定される場合、障害内容を示すレポート情報を生成することを特徴とする。

【 0 0 1 7 】

さらに、本発明では、障害に対して自社が対応できない場合、復旧作業の依頼を他社に通知する。

【 0 0 1 8 】

さらに、本発明では、前記第 1 タイプの機器は周辺機器であり、前記第 2 タイプの機器はコンピュータ機器であることを特徴とする。

【 0 0 1 9 】

さらに、本発明では、前記第 1 タイプの機器は、プリンタ、複写機、スキャナのうちの少なくとも一つであることを特徴とする。

【 0 0 2 0 】

さらに、本発明では、前記第 2 タイプの機器は、パーソナルコンピュータ、サーバコンピュータ、ネットワーク機器のうちの少なくとも一つであることを特徴

とする。

【0021】

【発明の実施の形態】

＜第1の遠隔サイト管理システムの構成＞

図を参照して本発明に係る遠隔サイト管理システムを説明する。

【0022】

図1は、遠隔サイト管理システムにおける被管理サイト（オフィス側）と管理サイト（保守サービス会社側）の構成を示すブロック図である。被管理サイトでは、汎用コンピュータであるPC103、デバイス監視サーバ203a（オフィスのローカルネットワーク上に接続されたデバイス系の周辺機器を管理する情報機器）、周辺機器である複写機101、プリンタ105、プリンタ104がLAN（ローカルエリアネットワーク）で接続されている。

【0023】

なお、ここでいう汎用コンピュータは、パーソナルコンピュータやサーバコンピュータのほか、ゲートウェイ、ルータなどのコンピュータネットワークに欠かせないネットワーク機器をも含むものとする。周辺機器は、複写機、プリンタ、スキャナー、FAX、複合機等を含むものとする。

【0024】

PC103では、後述するPC監視クライアントモジュールが実行され、これは、オフィスのローカルネットワーク上に接続された汎用コンピュータ機器等を管理することができる。また、デバイス監視サーバ203aとPC監視クライアントモジュールは物理的に別々のコンピュータで実行されてもよく、また一つのコンピュータで実行されても良い。

【0025】

また、図1に記載はされていないが、この遠隔サイト管理システムには、データフォーマット変換装置がある。これは、デバイス監視サーバ203aとPC監視クライアントモジュールとの間のデータフォーマット形式を変換・調整する装置である。

【0026】



また、管理サイトには、被管理サイトの機器を一元的に管理するためのセンタサーバ110、管理情報等を蓄積するためのインベントリデータベース109、被管理サイトにおける周辺機器の管理を専門に行うためのデバイスセンタサーバ210が、それぞれLANに接続されている。また、このシステムでは、サーバ・PC111といったその他のコンピュータが接続されている。このコンピュータ111では、管理情報を用いて、オフィス機器を統括管理するアプリケーションプログラムが実行されている。

## 【0027】

また、図1に記載はされていないが、管理サイトには、被管理サイトから通知されてくる情報を表示させる表示装置や、センタサーバ110とデバイスセンタサーバ210との間でデータフォーマット形式を変換・調整する変換装置もある。

## 【0028】

また、複数の管理サイトを統合的に管理するサービスセンタ（図2のアプリケーションシステム205に相当）もあり、これは、管理サイトと外部ネットワークまたはLANを介して接続されている。

## 【0029】

これら被管理サイトと管理サイトは、互いにゲートウェイ106、107で接続されている。この接続は、汎用のルータやモデム等を用いても良い。また、PC103においてPC監視クライアントモジュールが実行されている場合には、PC103とセンタサーバ109との間の回線と、デバイス監視サーバ203aとデバイスセンタサーバ210との間の回線が、それぞれ別々に設けられ、それぞれ独立していてもよい。

## 【0030】

図3は、PC及びサーバコンピュータの構成を示すブロック図である。図3において、コンピュータ3000は、CPU1、RAM2、ROM3、システムバス4、KBC5、CRTC6、MC7、LAN制御部8、KB9、CRT10、外部メモリ11とを備える。

## 【0031】

CPU1は、ROM3のプログラム用ROMに記憶された通信制御プログラムを実行して、それに基づいて、指定されたデータの外部への送信を制御したり、あるいは外部からのデータの受信を制御したりする。また、CPU1は、システムバス4に接続される各デバイスを統括的に制御する。

#### 【0032】

RAM2は、CPU1の主メモリ、ワークエリア等として機能する。ROMは、それぞれフォント（フォントROM）、プログラム（プログラムROM）、データ（データROM）を記憶する。キーボードコントローラ（KBC）5は、キーボード9や不図示のポインティングデバイスからのキー入力を制御する。CRTコントローラ（CRTC）6は、CRTディスプレイ10の表示を制御する。メモリコントローラ（MC）7は、外部メモリ11へのアクセスを制御する。ハードディスク（HD）やフロッピーディスク（FD）等の外部メモリ11は、ブートプログラム、種々のアプリケーション、フォントデータ、ユーザファイル、後述する編集ファイル等を記憶する。LAN制御部8は、ネットワークに接続されて、ネットワークに接続された他の機器との通信処理を実行する。

#### 【0033】

図2は本遠隔サイト管理システムのソフトウェアモジュールの構成を示すブロック図である。ユーザ拠点システム（被管理サイトを指す）では、デバイス系機器（複写機、プリンタ、複合機、スキャナ、FAX等の周辺機器）と、PC・サーバ系機器（汎用コンピュータなど）が混在している。が、デバイス系機器はデバイス監視サーバ203aによって、PC・サーバ系機器はPC監視クライアントモジュール203dによってそれぞれローカルで管理される。これらを総称して、拠点側管理システム203と呼ぶことにする。デバイス監視サーバ203aは、管理情報を蓄積するためのデータベース203a-1を有する。

#### 【0034】

一方、センターシステム（管理サイトを指す）は、デバイス監視サーバ203aとの間でデータを交換するデバイスセンタサーバ210と、PC監視クライアントモジュール203dとの間でデータを交換するセンタサーバ110とを含む。デバイス系機器の管理情報はインベントリデータベース109に蓄積される。

また、センタサーバ110によって管理される管理情報もインベントリデータベース109に蓄積される。これらインベントリデータベース109に蓄積される管理情報は、アプリケーションシステム205等により利用される。なお、インベントリデータベース109はデバイス系とPC・サーバ等の汎用コンピュータ系とで、それぞれ論理的に分かれていればよく、無論、物理的に分かれていてもよい。

## 【0035】

デバイス監視サーバ203aとデバイスセンタサーバ210とは、データ形式や手順を必要に応じて変換するための拠点プラグインモジュール203bとサーバプラグインモジュールを介して接続されている。これら拠点プラグインモジュールとサーバプラグインモジュールとによって、拠点側とセンタ側とで使用OSが異なる場合などでも、お互いの通信が可能になる。また、電氣的には、ルータ204を介する。この回線は、PC監視クライアント203dとセンタサーバ110とを接続する回線と物理的または論理的に共用されている。

## 【0036】

デバイスセンタサーバ210とデバイス監視サーバ230aを接続する回線は、監視クライアント203dとセンタサーバ間を接続する回線と共用されない場合も想定される。その場合には、モデムやルータを介して、管理クライアント203d-センタサーバ110とは独立した回線で接続されても良い。

## 【0037】

センタサーバ110には、イベントモニタ110aが含まれており、センタサーバ110に対して発行されたイベントを監視し、障害の発生等を伝えるイベントであればモニタ上に表示する。管理者はその表示を見ることで、被管理サイトにおいて発生した障害の状況を知ることができる。センタサーバ110に対してイベントを発行するのは、イベントアダプタ210aと、PC監視クライアント203dと、アプリケーションシステム205である。センタサーバ110は、受け取ったイベントを、それが示す内容に従って所定の処理を実行する。イベントとしては例えば、障害通知等がある。

## 【0038】

デバイスセンタサーバ210には、イベントアダプタモジュール210aが含まれている。イベントアダプタ210aは、デバイス監視サーバ203aからデバイスセンタサーバ210に対して送られてきて受信した情報を定期的に検索する機能を持ち、その検索された情報の内から、周辺機器において発生した障害に関する情報を判別してより分けて、センタサーバ110において処理可能な形式（ファイル形式、プロトコル形式等）に変換してから、センタサーバ110に対して障害の発生を示すイベントを発行する。あるいは、イベントアダプタモジュール210aによってセンタサーバに処理可能な形式に変換する機能をセンタサーバ110に持たせてもよい。障害関連のイベント（障害イベント）には、障害の起きた装置やその内容、発生時刻等が含まれる。このイベントアダプタ210aを本システム及び装置に設けることによって、デバイス専用想定されたプロトコル・フォーマットを使用した管理ソフトによって得られたデバイス固有の情報、例えば、紙詰まり、ステープル機能チェック等を別の種別のシステム・装置（実施例では汎用コンピュータ・サーバ等）を監視するソフトと一元化して管理することが可能となる。

## 【0039】

イベントモニタ110aはそれを受けて、障害の起きた装置やその内容、発生時刻等を、イベントのリストに加えて表示する。表示の方法としては、たとえば、1行に1イベントを表示し、時系列的にイベントのリストを表示する。図2ではイベントモニタ110aはセンタサーバ110に含まれる形で記載されているが、このイベントモニタ110aをセンタサーバ110からネットワーク等を介して外部に接続することで、例えば、デバイスセンタサーバ210側やアプリケーションシステム205側でデバース系、PC・サーバ系を包括管理することが可能となる。

## 【0040】

ここで注意すべきなのは、イベントモニタ110aは、イベントの発生元を意識することなく、障害系のイベントであればそれを表示することで、管理者の注意を喚起できる、ということである。すなわち、イベントモニタ110aにおいては、PC監視クライアント203dから発行された、汎用コンピュータ系の障

害イベントと、デバイスセンタサーバ210のイベントアダプタ210aを介してデバイス監視サーバ203aから発行された、周辺機器系の障害イベントとを、同一画面上のイベントリストにたとえば時系列的に表示する。

#### 【0041】

次に、デバイスセンタサーバ210と、デバイス監視サーバ203aとの間でなされるデータ交換の手順の例を、図4を参照しつつ、(1)デバイスへの、デバイスセンタサーバ210からの設定値のダウンロード、(2)デバイス監視サーバ203aからデバイスセンタサーバ210へのログデータのアップロード、(3)デバイスセンタサーバ210からデバイス監視サーバ203aへのカウンタデータの要求、という3つのケースで説明する。その前に、データフォーマットについて簡単に説明する。

#### 【0042】

図8は、デバイスセンタサーバ210とデバイス監視サーバ203aとの間で交換されるメッセージフォーマットの一例を示す図である。1つのメッセージは、フラグフィールド、データ種別フィールド、ジョブIDフィールド、リターン値フィールド、データ長フィールド、データフィールドを含む。フラグフィールドには、通信手段を示すビット群と、そのメッセージがデータの最終フレームであるか否かを示すビットが含まれる。

#### 【0043】

データ種別フィールドでは、たとえば認証要求データ（セッションの先頭に送信されるデータ）であることや、ダウンロードされる設定値データであること、後述するデバイス情報要求であること、イベント情報の通知であること、ログデータ処理要求であることなどが示される。たとえば障害の通知などは、イベント情報であることがデータ種別として示され、データフィールドで具体的な内容が示される。

#### 【0044】

ジョブIDは、そのセッションの種類を示すもので、パラメータ設定やデバイス情報の取得、イベント通知などがこれによって示される。データ長には後続するデータの長さが示され、データフィールドには、データ長で示された長さのデ

ータが格納される。設定値のダウンロードやログデータの処理要求には、データフィールドにデータが載せられる。また、カウンタアップロードにおいては、デバイス情報要求に対する応答のデータフィールドに、デバイス情報が載せられる。

【0045】

以下の手順をはじめ、デバイスセンタサーバ210やデバイス監視サーバ203aは、このメッセージを交換しつつ処理を遂行する。なお、以下の説明では、イベントとは、イベントの発生を伝えるためのメッセージという意味で使用している。

【0046】

<設定値ダウンロード手順>

図4は、拠点システムとセンタシステムとの間で行われる、データの交換の手順を説明するためのブロック図である。

【0047】

設定値のダウンロードは次のようにして行われる。

【0048】

(1) アプリケーションシステム205において、手作業などで、設定対象のデバイスの指定やデバイスのIPアドレス、デバイスの拠点デバイスサーバに対するエラー等のアラーム通知の時の閾値の設定値等を入力し、設定値情報ファイル401を作成する。

【0049】

(2) アプリケーションシステム205よりデバイスセンタサーバ210との間のセッションを確立し、設定値情報ファイル401に含まれる設定値データを送信する。

【0050】

(3) デバイスセンタサーバ210は、設定値データを受信すると、デバイス監視サーバ203aとの間でセッションを確立し、デバイス監視サーバ203aに対して設定値データを送信する。

【0051】

(4) デバイス監視サーバ203aは、設定値データを受信するとデバイスに設定値を送りつける。この手順は、デバイスごとに定まった手順で行われる。

【0052】

(5) デバイスの設定が終了すると、デバイス監視サーバ203aは、デバイスセンタサーバ210に対して設定終了を送信する。

【0053】

(6) デバイスセンタサーバ210は、アプリケーションシステム205に対して設定終了通知を送信する。

【0054】

その後、アプリケーションシステム205はデバイスセンタサーバ210との間のセッションを解放し、デバイスセンタサーバ210は、デバイス監視サーバ203aとの間のセッションを解放する。

【0055】

以上のようにして、デバイス監視サーバ203aとデバイスセンタサーバ210とは直接通信することで、デバイスの設定情報をデバイス402にダウンロードする事ができる。

【0056】

なお、障害に関しては次のようになる。

【0057】

(7) PC監視クライアント203dがサーバやPCにおいて何らかの障害を検出し、障害イベントを発行する際には、センタサーバ110に対して直接イベントを発行する。

【0058】

(8) また、デバイス監視サーバ203aがデバイス402の障害を検出した場合には、その情報をデバイスセンタサーバ210に送信する。

【0059】

(9) デバイスセンタサーバ210は、デバイス402における障害の通報を受信すると、それを基に、センタサーバ110に対して障害発生を知らせるイベントを発行する。図4のデバイスセンタサーバ210には図2のイベントアダプ

タ 201 a が含まれる形で記載されおり、イベントアダプタ 201 a から図 4 に記載される障害系イベントが発行されることになる。

【0060】

(10) イベントモニタ 110 a は、そのイベントが障害系イベントであるので、イベントコンソールにその障害情報を表示させ、イベントリストを更新する。

【0061】

このように、障害を通知するイベントは、被管理サイトのどのデバイス系または汎用コンピュータ系で生じても、センタサーバ 110 を通ることになり、管理者は、センタサーバのイベントコンソールを監視するだけで、被管理サイトのすべてのデバイス系の情報または汎用コンピュータ系の情報を監視できる。また、イベントコンソールに表示される情報は、印刷出力されたり、サービスマンの所持する形態端末等に表示されるような処理を施されることも考えられる。印刷された情報は、被管理者宛に郵送で送られたり、サービスマンの形態端末に表示された情報はサービスマンの派遣等に利用することができる。このようにデバイス系と汎用 PC・サーバ系を一元管理された情報を様々な形態で応用する場面が想定される。

【0062】

前述の記載では、デバイス系の障害を図 4 中のイベントモニタ 110 a を介してイベントコンソール 110 b に表示させることについて説明してきたが、本発明の特徴として、デバイス系で発生した全ての障害情報をイベントコンソール 110 b に表示するわけではないことが挙げられる。すなわちデバイス機器の障害のレベルによってデバイスセンタサーバ 210 に情報を送信するか否かの判断処理を行う機能を本システムは有する。

【0063】

例えば、複写機等におけるドアオープンエラー、デバイス機器のパワーオン・オフ機能によるリセットで回復できるようなエラーに関してはデバイス監視サーバ 203 a はデバイスセンタサーバ 210 にエラー通知を行わない。一方、センタサーバに通知されてくる情報のうちでも、顧客先で顧客による対応がとれるエ



ラー、例えば、デバイスの温度上昇等の現状動作に支障の無いエラー、ジャムエラー) に関しては、サービスマンの呼び出し等を行わない。

【0064】

これら、センタサーバへ障害を通知するか否かの判断機能データベースは監視データベース203a-1、デバイス402、等のデバイス側の機器のいずれかに記憶されていれば、デバイス側からセンタ側に情報を通知するか否かの判断を行うことができる。

【0065】

また、センタサーバ110に通知されてきた障害情報をイベントコンソール110bに表示するか否か、または、サービスマンに連絡するか否かの判断機能データベースはセンタサーバ側のアプリケーションシステム209、インベントリデータベース109、センタサーバ110等の機器のいずれかに記憶されていれば、本発明の機能を達成することはできる。

【0066】

これらの情報伝達に伴うフィルタリング機能を本システムは有することにより、拠点側－センタ側間のトラフィック量の軽減、また、センタ側で管理する管理者にとって、重大なエラー情報をより明確且つ容易に認識することが可能となる。

【0067】

<カウンタアップロード手順>

カウンタ値のアップロード、すなわちデバイス情報の収集は次のようにして行われる。カウンタ値とは、複写機やプリンタにおいて印刷したページ数を示す値、デバイスの各種モードがどれほど使用されたかを示すモードカウンタ等であり、保守料金算定の基本となる値である。これをセンタシステムからの要求に応じてアップロードすることで、遠隔サイトからのカウンタ値をはじめとするデバイス情報の取り込みを可能とする。カウンタのアップロードはアプリケーションからの要求に応じて行われるために、センタシステム(管理サイト)がイニシエータとなる。

【0068】

(1) アプリケーションシステム205よりセッションを確立し、デバイス情報要求をデバイスセンタサーバ210に対して送信する。デバイス情報要求には、拠点システムにおける対象デバイスを指定する情報等が含まれている。

【0069】

(2) デバイスセンタサーバ210は、デバイス情報要求を受信すると、デバイス監視サーバ203aとの間でセッションを確立し、デバイス監視サーバ203aに対してデバイス情報要求を送信する。

【0070】

(3) デバイス監視サーバ203aは、デバイス情報要求を受信すると、デバイス情報を指定されたデバイスから取得する。この手順は、デバイスごとに定まった手順で行われ、デバイスごとに定まった情報、あるいは指定された情報が取得される。

【0071】

(4) デバイス情報を取得すると、デバイス監視サーバ203aは、デバイスセンタサーバ210に対して取得したデバイス情報を含むデバイス情報応答を送信する。

【0072】

(5) デバイスセンタサーバ210は、アプリケーションシステム205に対してデバイス情報応答を送信する。

【0073】

その後、アプリケーションシステム205はデバイスセンタサーバ210との間のセッションを解放し、デバイスセンタサーバ210は、デバイス監視サーバ203aとの間のセッションを解放する。

【0074】

以上のようにして、デバイス監視サーバ203aとデバイスセンタサーバ210とは直接通信することで、デバイス情報を取得することができる。

【0075】

なお、障害に関しては設定値のダウンロードと同じ要領で行われる。

【0076】

＜ログデータアップロード手順＞

ログデータのアップロードは次のようにして行われる。ログデータとは、たとえば周辺機器において発生した警告やリトライの情報などが履歴で、それらの警告が所定回数以上に達するなど、エラーに至らないまでも、何らかの異常事態が発生しつつあることが予想される場合にそれを管理サイトに自発的に送信する。したがって、ログデータのアップロードはカウンタのアップロードとは異なり、被管理サイト（拠点システム）がイニシエータとなる。

【0077】

(1) デバイス監視サーバ203aがデバイスのログを収集する。その量が所定値を越えたり、警告の発生頻度が所定の率を超えた場合には、デバイス監視サーバ203aはログデータのアップロードを開始する。

【0078】

(2) まず、デバイス監視サーバ203aよりセッションを確立し、ログデータを含むログデータ処理要求をデバイスセンタサーバ210に対して送信する。

【0079】

(3) デバイス監視サーバ203aは、ログデータ処理要求を受信すると、デバイスセンタサーバ210との間でセッションを確立し、デバイスセンタサーバ210に対してログ処理要求を送信する。

【0080】

(4) デバイスセンタサーバ210は、ログデータ処理要求を受信すると、アプリケーションシステム205との間にセッションを確立し、ログデータ処理要求を、ログデータを処理するアプリケーションシステム205に対して送信する。

【0081】

(5) アプリケーションシステム205は、ログデータ処理要求を受信すると、それと共に受信したログデータを処理し、ログデータ処理応答を、デバイスセンタサーバ210に対して送信する。

【0082】

(6) デバイスセンタサーバ210は、デバイス監視サーバ203aに対して

ログデータ処理応答を送信する。

【0083】

(7) デバイス監視サーバ203aは、デバイスセンタサーバ210との間のセッションを解放し、後処理を行う。後処理においては、ログデータ処理応答が、ログデータの処理が正常に完了したことを示すものであれば、ログデータ消去などを行う。

【0084】

その後、デバイスセンタサーバ210はアプリケーションシステム205との間のセッションを解放する。

【0085】

以上のようにして、デバイス監視サーバ203aとデバイスセンタサーバ210とは直接通信することで、ログ情報をアップロードすることができる。

【0086】

なお、障害に関しては設定値のダウンロードと同じ要領で行われる。

【0087】

＜デバイスセンタサーバによる処理手順＞

次に、デバイスセンタサーバ210、デバイス監視サーバ203aそれぞれにおける処理手順を簡単に示す。図5は、デバイスセンタサーバにおけるメッセージ受信時の処理手順を示すフローチャートである。なお、このメッセージはデバイス監視サーバからのものとは限らず、アプリケーションシステム205からも受信する。このメッセージのフォーマットは、図8と異なるものでも良い。いずれにしても、メッセージの発信元を識別可能にできているか、あるいは、発信元に応じて異なるプロセスが実行される。本実施形態では、前者を採用する。

【0088】

メッセージを受信すると、図5の処理が開始される。まず、受信したメッセージを解析し（ステップS501）、その発行元が判定される（ステップS502）。発行元は、アドレス等をメッセージに付加しても良いが、その内容によっても識別できる。たとえば、ログ処理要求であれば、その発行元はデバイス監視サーバであり、設定値ダウンロード要求であればアプリケーションシステム（フロ

ーチャートではバックエンドと示している)である。

【0089】

発行元がデバイス監視サーバ203aであれば、それが障害イベントであるか判定し(ステップS503)、障害イベントであれば、センタサーバ110へ処理可能な形式に変換してから転送する(ステップS504)。センタサーバ110においては障害の場所や内容、時刻などがそのメッセージに含まれたデータから読み出され、表示される(ステップS505)。障害イベントでない場合には、データをアプリケーションシステムに渡してメッセージに応じた処理をさせ、メッセージ待ちとなる。アプリケーションシステムに渡す処理には、たとえばログデータ処理要求や、収集されたデバイス情報が含まれる。

【0090】

一方、発行元がアプリケーションシステムであれば、そのメッセージがデバイス情報の収集要求であるか判定する(ステップS506)。そうであれば、デバイス情報収集要求をデバイス監視サーバ203aに対して発行し、メッセージ待ちとなる。

【0091】

デバイス情報収集要求でなければ設定値のダウンロード要求であるかが判定される(ステップS508)。ダウンロード要求であれば、受信したダウンロード情報を取得し(ステップS509)、それをデバイス監視サーバ203aに対して発呼する(ステップS510)。

【0092】

＜デバイス監視サーバによる処理手順＞

図6は、デバイス監視サーバ203aにおいて発生したイベントに対する処理手順を示すフローチャートである。

【0093】

何らかのイベントが発生すると、発生したイベントを解析し(ステップS601)、それがデバイスからの警告であり、所定の閾値を越えていれば(ステップS602)、それまでに蓄積したログデータを取得してログデータ処理要求のメッセージを作成し(ステップS603)デバイスセンタサーバ210に対してロ

グ処理要求を発行する。閾値を超えていなければログに蓄積する。

【0094】

一方、警告でなければ本実施例ではエラーの発生であるとみなして障害イベントを示すメッセージを作成し（ステップS605）、ステップS604でデバイスセンタサーバ210に送信する。

【0095】

図7は、デバイス監視サーバ203aが、デバイスセンタサーバ210から受信したメッセージを受信する手順を示すフローチャートである。

【0096】

まず、受信したメッセージが設定値のダウンロード要求であるか判定する（ステップS701）。ダウンロードであれば、受信した設定値データに基づく設定をデバイス監視サーバ203aとデバイス間で。 （ステップS702）、拠点プラグイン203bがそのデータを削除し（ステップS703）、デバイスセンタサーバ210に対してダウンロードが完了した旨の応答メッセージを発行する（ステップS704）。なお、拠点プラグイン203bはデバイス監視サーバ203aに論理的に接続されていればよく、接続されていれば物理的に分かれていてもよい。

【0097】

ダウンロードでなければ、デバイス情報収集要求であるか判定し（ステップS706）、そうであれば指定されたデバイスから情報を収集して（ステップS707）、デバイスセンタサーバにそのデバイス情報を送信する（ステップS708）。

【0098】

以上の手順により、汎用コンピュータのための管理システムと、周辺機器のための管理システムとによる障害イベントを、管理サイト側においては統合された情報として一元的に管理できる。また、本発明はPC・サーバ系の管理ソフトにデバイス系の管理情報を適合させるものに限定されるものではなく、その逆、即ちデバイス系の管理ソフトにPC・サーバ系の管理情報を適合させるものにすることも可能である。例えば、図2中のイベントアダプタ210aをセンタサーバ

1 1 0 に設けて、デバイスサーバで発生したイベントをデバイスセンタサーバ 2 1 0 に通知するようにしてもよい。

【0 0 9 9】

また、図 2 に示したように、デバイス監視サーバ 2 0 3 a とデバイスセンタサーバ 2 0 1 とを接続する回線と、P C 監視クライアント 2 0 3 d とセンタサーバ 1 1 0 とを接続する回線とを同じ回線とし、ルータ等で共用することで、回線数の節約を図ることもできる。これは回線として専用回線を使用する場合などに有効である。

【0 1 0 0】

<第 2 の遠隔サイト管理システムの構成>

図を参照して本発明の第 2 の実施形態である遠隔サイト管理システムを説明する。本実施形態のシステムは、第 1 の実施形態のそれと比較して、管理サイトと被管理サイトとの間における論理的なチャネルの持ち方において相違する。第 1 の実施形態においては、通信回線を共用することは可能であるものの、デバイス監視サーバ 2 0 3 a とデバイスセンタサーバ 2 1 0 とを接続するチャネルと、P C 監視クライアント 2 0 3 d とセンタサーバ 1 1 0 とを接続するチャネルとは、論理的には互いに独立した別個のチャネルである。デバイスセンタサーバ 2 1 0 が障害イベントの通知をデバイス監視サーバ 2 0 3 a から受信した場合に、障害の発生を通知するイベントをセンタサーバ 1 1 0 に送信することで、イベントモニタにおける障害イベントの一元化が図られている。

【0 1 0 1】

これに対して本実施形態では、デバイスセンタサーバ 2 1 0 も、デバイス監視サーバ 2 0 3 a とデバイスセンタサーバ 2 0 1 とを接続するチャネルも存在しない。デバイスセンタサーバの代わりに、デバイス情報処理モジュール 9 0 1 がセンタサーバ 1 1 0 におかれ（図では別体として示した）、センタサーバ 1 1 0 が受信したデバイス系の情報を処理している。この構成においては、市販の P C 監視クライアント 2 0 3 d とセンタサーバ 1 1 0 とを用いた場合に、その間に確立されるチャネルに、デバイス系のメッセージも流してしまう。こうすることで、第 1 実施例で説明したように回線を共通に使用できるメリットの他に、デバイス

系の情報のために独立した通信チャネルを用意する必要がなく、デバイスセンタサーバを別途設ける必要もなくなるという効果を得ることができる。

#### 【0102】

##### ＜システム構成＞

図9は、本実施形態の遠隔サイト管理システムのソフトウェアモジュールの構成を示すブロック図である。ユーザ拠点システム（被管理サイトを指す）は、デバイス系機器（プリンタ、複写機、スキャナー、FAX、複合機等の周辺機器）と、PC・サーバ系機器（汎用コンピュータ）が混在しているが、デバイス系機器はデバイス監視サーバ203aによって、PC・サーバ系機器はPC監視クライアント203dによって管理される。この点は第1の実施形態と同様である。

#### 【0103】

センターシステム（管理サイトを指す）は、デバイス監視サーバ203aとの間でデータを交換するデバイス情報処理モジュール901と、PC監視クライアント203dとの間でデータを交換するセンタサーバ110とを含む。デバイス系機器およびPC・サーバ系の管理情報はインベントリデータベース109に蓄積される。図9では一つのデータベースとして図示されているが、論理的または物理的にデバイス系とPC・サーバ系のデータベースが分かれていればよい。この情報はアプリケーションシステム205、センタサーバ110等により利用される。これも第1の実施形態と同様である。

#### 【0104】

管理サイトと被管理サイトとは、ルータ204同士で接続された一本の回線で接続されている。このPC監視クライアント203dとセンタサーバ110とは市販のサイト管理システムで実現できる。すべてのメッセージは、この市販の管理システムにより提供される、PC監視クライアント203dとセンタサーバ110とで構成されるチャネルを通して送受信される。なお、図9ではデバイス情報処理モジュール901が独立してあるものとして（図2のデバイスセンタサーバ210に相当）いるが、この機能をセンタサーバ110に組み込んで実現することもできる。

#### 【0105】



デバイス監視サーバ203aとPC監視クライアント203dとは、データ形式（フォーマット）や手順（プロトコル）を必要に応じて変換するための拠点プラグインモジュール203bを介して接続されている。すなわち、デバイス監視サーバの情報をPC監視クライアント203aのフォーマット（またはプロトコル）に変換する機能、その逆の変換の機能を拠点プラグインモジュール203bは有している。また、センタ側でセンタサーバ110とデバイス処理モジュール901間でのデータを受け渡しを行うセンタ側のプラグイン（図2のサーバプラグインに相当）に、この拠点プラグインモジュール203bと同等の機能を持たせることも考えられる。

#### 【0106】

この拠点プラグインモジュール203bは、後述するように、PC監視クライアント203dに対してデバイス監視サーバ203aからのメッセージを渡して指定した宛先に送信させると共に、PC監視クライアント203dが書き込む所定のデータ領域の内容を定期的にポーリングし検索を行い、デバイス監視サーバ203a宛のメッセージがあればそれをデバイス監視サーバ203aに渡す役割を有する。

#### 【0107】

また、センタサーバ110は、受信したメッセージに応じて、そのメッセージの内容がデバイスに係る情報であればデバイス情報処理モジュールに渡して処理をさせるし、イベントの発生を知らせるメッセージであれば、イベントモニタ110aにより発生したイベントをデバイス系のイベントかPC・サーバ系のイベントかを識別可能な表示形態にしてイベントリストとして表示させる。デバイス系のイベントについてはデバイス情報処理モジュール901から発生されることになる。

#### 【0108】

このように、デバイス系とPC・サーバ系間のフォーマット変換機能を有するプラグインを設ける事により、市販されているPC・サーバ系の管理ソフトの機能を流用することが可能となり、デバイス系の情報を拠点側と管理センタ側で送受信をすることができる。また、市販のPC・サーバ系の管理ソフトでは詳細に

管理できないような、デバイス固有の情報に関しても、センタ側で送信されてきたデバイス系のない様々に係るデータをPC・サーバ系のフォーマットからデバイス系のフォーマットに変換してからデバイス情報処理モジュールで処理をすればよく、デバイスの情報を詳細に管理したい場合には、デバイス情報処理モジュールのみを独自に開発すればよく、開発・設計の効率を上げる効果を得ることができる。

## 【0109】

次に、拠点システム（被管理サイト）と、センタシステム（管理サイト）との間でなされるメッセージ交換の手順の例を、図10乃至図12を参照しつつ、（1）デバイスへの、デバイスセンタサーバ210からの設定値のダウンロード、（2）デバイス監視サーバ203aからデバイスセンタサーバ210へのログデータのアップロード、（3）デバイスセンタサーバ210からデバイス監視サーバ203aへのカウンタデータの要求、という3つのケースで説明する。

## 【0110】

## ＜設定値ダウンロード手順＞

図10は、拠点システムとセンタシステムとの間で行われる、デバイスへの設定値のダウンロードの手順を説明するためのブロック図である。設定値のダウンロードは次のようにして行われる。

## 【0111】

まずアプリケーションシステム205において、手作業などで、設定対象のデバイスの指定や設定値等を入力し、設定値情報ファイル1002を作成しておく。

## 【0112】

（1）アプリケーションシステム205よりセンタサーバ110との間のセッションを確立する。

## 【0113】

（2）センタサーバ110において配布モジュール1001を起動し、設定値情報ファイル1002から配布用ファイルパッケージ1001aを作成する。

## 【0114】

(3) 配布モジュール1001aは、配布用パッケージファイルをPC監視クライアント203dに送信し、ワークファイルとして格納させる。

【0115】

(4) 拠点プラグイン203bは、PC監視クライアント203dが格納するデータファイルを定期的に監視しており、PC監視クライアントによりワークファイルが作成されたことを検知すると、デバイス監視サーバに設定値の到着を通知すると共に、設定値データをデバイス監視サーバ203aに渡す。デバイス監視サーバ203aは、指定されたデバイスに、設定された値を設定する。

【0116】

(4-2) 拠点プラグイン203bは、PC監視クライアント203dを介してセンタサーバに設定が終了したことを通知する。

【0117】

(5) センタサーバ110では、配布モジュール1001により、配布用パッケージファイル1001aを削除させる。

【0118】

(6) センタサーバ110は、アプリケーションシステム205に対して設定の終了を通知する。

【0119】

以上のようにして、デバイス監視サーバ203aに設定データを渡すことで、デバイスの設定情報をデバイスにダウンロードすることができる。

【0120】

なお、デバイス系で発生した障害に関しては、上記手順(4-2)と同様にして拠点プラグイン203bからPC監視クライアント203dを介してセンタサーバ110に障害イベントとして送信する。このために、障害を通知するイベントは、センタサーバ110のイベントモニタ110aで処理され、イベントのリストに表示される。

【0121】

<カウンタアップロード手順>

図11は、拠点システムとセンタシステムとの間で行われる、カウントデータ

のアップロード、すなわちデバイス情報収集の手順を説明するためのフローチャートである。デバイス情報のアップロードは次のようにして行われる。

【0122】

(1) アプリケーションシステム205は情報要求コマンドをファイルに格納し、センタサーバ110に対して情報収集のきっかけとなるメッセージ（イベント）を発行する。

【0123】

(2) アプリケーションシステム205からのイベントをイベントモニタが解析し、配布モジュール1001を起動して、情報要求コマンドの配布用ファイルパッケージ1001aを作成する。

【0124】

(3) センタサーバ110は、作成した情報要求コマンドを含む配布用パッケージをPC監視クライアント203dに対して送信する。PC監視サーバ203dは受信したファイルをワークファイルとして格納する。なお、ワークファイルはPC・サーバ管理システムでの汎用ファイルなるもので、配布用ファイルパッケージ1001aの実態に該当するものである。

【0125】

(4) 拠点プラグイン203bは、PC監視サーバ203dがファイルを格納したことを検知すると、それを呼んでデバイス監視サーバ203aに渡す。デバイス監視サーバ203aは、それを受けて指定されたデバイスから、デバイス情報を収集して拠点プラグイン203dに渡す。

【0126】

(5) 拠点プラグイン203bは、受信したデバイス情報を、所定の形式のファイル203eとして格納する。本実施例では以下に所定の形式としてMIF形式を例に説明を進めていくが、MIF形式とは情報管理系の一般的なファイル形式を指す。

【0127】

(6) 拠点プラグイン203bは、ワークファイルを削除する。

【0128】

(7) 拠点プラグインは、MIFファイルを作成した旨のイベントを作成してセンタサーバ110に送信する。

【0129】

(8) センタサーバ110はそのイベントを受け、配布用ファイルパッケージを削除する。

【0130】

(9) また、センタサーバ110は、拠点プラグイン203bから受信したイベントが、正常な情報収集の完了を通知するものであれば、共通情報収集モジュール1102を起動し、拠点プラグインの作成したMIFファイルを読み込ませてデバイス情報を収集させる。

【0131】

(10) 共通情報収集モジュール1101は、MIFファイル203eを読み、収集したデバイス情報を獲得する。

【0132】

(11) 共通情報収集モジュール1101は獲得したデバイス情報をインベントリデータベースに格納する。なお、インベントリデータベースは物理的または論理的にデバイス機器系とPC・サーバ機器系のデータベースとをそれぞれ有しており、対象機器に応じて柔軟な処理を行うことができる。

【0133】

(12) センタサーバは拠点側のMIFファイル203eを削除させる。

【0134】

(13) アプリケーションに完了通知を送信する。

【0135】

以上のようにして、デバイス監視サーバ203aが収集したデバイス情報をセンタサーバ110に取得することができる。

【0136】

<ログデータアップロード手順>

図12は、拠点システムからセンタシステムへのログデータのアップロード手順を説明するためのフローチャートである。ログデータのアップロードは本実施

形態では次のようにして行われる。

【0137】

(1) デバイス監視サーバ203aは、拠点プラグインに203bに対して、エラーや警告、それらの回数が閾値を超えたことを検知した旨の通知を発行する。

【0138】

(2) デバイス監視サーバ203aは、拠点プラグインに203dに対して前述した警告のイベントデータ発行する。

【0139】

(3) 拠点プラグイン203bは、ログデータを、MIF形式のファイル203eとして格納する。MIF形式とは、前述で説明したとおり、情報管理系の一般的なファイル・データ形式である。

【0140】

(4) 拠点プラグイン203bは、MIFファイルを作成した旨のイベントを作成してセンタサーバ110に送信する。

【0141】

(5) センタサーバ110はそのイベントを受け、共通情報収集モジュール1201を起動する。

【0142】

(6) 共通情報収集モジュール1201は、拠点プラグイン203bの作成したMIFファイル203eを読み込ませてログファイルを読む。

【0143】

(7) 共通情報収集モジュール1101は、獲得したデバイス情報をインベントリデータベース109に格納する。

【0144】

(8) センタサーバは拠点側のMIFファイル203eを削除させる。

【0145】

(9) アプリケーションに完了通知を送信する。

【0146】

以上のようにして、デバイス監視サーバ203aが作成したログデータファイルをセンタサーバ110は取得することができる。

## 【0147】

## ＜デバイスセンタサーバによる処理手順＞

次に、センタサーバ110、デバイス情報処理モジュール901、拠点プラグイン203b、PC監視クライアント203dによる処理手順を簡単に示す。図13は、センタサーバ110におけるイベント受信時の処理手順を示すフローチャートである。イベントを受信すると、図13の処理が開始される。なお、以下の説明において、メッセージとイベントは厳密に区別されていない。イベントとは、イベントの発生を伝えるメッセージ、という意味で使用している。

## 【0148】

まず、受信したイベントを解析し（ステップS1301）、その発行元が判定される（ステップS1302）。発行元がPC監視クライアント203dであれば、イベントモニタにより処理されて、障害イベントであればイベントリストに表示される（ステップS1303）。

## 【0149】

そのあとで、イベントがデバイス系であるか否か、すなわちそれが拠点プラグイン203bから発行されたものか否かが判定され（ステップS1304）、デバイス系であれば、イベントごとに応じてデバイス情報処理モジュールにより処理が行われる。この手順が図14乃至図16に示されている。デバイス系でなければ、センタサーバ110によりイベントに応じた処理が行われる。

## 【0150】

一方、イベントの発行元がバックエンド、すなわちアプリケーションシステムであれば、そのイベントが情報収集を行わせるためのものが判定され（ステップS1305）、そうであれば、情報収集要求を拠点プラグインモジュール203bに対して発行する（ステップS1309）。情報収集要求は、その要求を行うための配布モジュール1001に配布用ファイルパッケージを作成し、それを配布させて行わせる。

## 【0151】

情報収集要求のイベントでなければ、ダウンロードを要求するためのイベントであるか判定する（ステップS1306）。そのイベントでもなければ、イベントに応じた処理をおこなってイベント待ちとなる。

## 【0152】

ダウンロード要求の場合には、ダウンロードするデータをバックエンドから獲得し（ステップS1307）、ダウンロードデータを拠点プラグイン203bに対して配布する（ステップS1308）。

## 【0153】

## ＜デバイス情報処理モジュールによる処理手順＞

図13のステップS1304でデバイス系と判定されたイベントは、更に詳細に分析されて、（1）ダウンロード終了の通知イベント、（2）デバイス情報収集終了のイベント、（3）ログデータアップロードの要求のイベント、という3種の処理に分岐する。これらの処理は、それぞれ図14乃至図16のフローチャートの手順となる。

## 【0154】

## （ダウンロード終了）

図14は、デバイス情報処理モジュール901による、ダウンロード終了イベントに対する処理手順を示すフローチャートである。ダウンロードの終了が通知されると、まず配布ファイルパッケージ1001aを削除し（ステップS1401）、ダウンロードが終了したことをバックエンドに通知する（ステップS1402）。

## 【0155】

## （デバイス情報の取得）

図15は、デバイス情報処理モジュール901による、デバイス情報取得（カウンタアップロード）の通知に対する処理手順を示すフローチャートである。

## 【0156】

まず、情報収集要求のために作成した配布用ファイルパッケージ1001aを削除する（ステップS1501）。次に、データの取得が正常に行われていれば、情報収集モジュール11101を起動し（ステップS1503）、デバイス監



視サーバ203aに対してデバイス情報の格納されたMIFファイルを要求し、それに対する応答であるMIFファイルを受信する（ステップS1504）。

【0157】

そして受信したファイルをインベントリデータベース109に格納し（ステップS1505）、デバイス監視サーバ203aに対してMIFファイルの削除を要求する（ステップS1506）。最後にバックエンドに対してデバイス情報の収集が終了したことを通知する（ステップS1507）。

【0158】

一方、ステップ1502で正常でないと判定された場合には、その旨をバックエンドに対して通知する（ステップS1508）。

【0159】

以上のようにして、MIFファイルとして作成されたデバイス情報をデバイス監視サーバ203aから取得する。

【0160】

（ログデータアップロード）

図16は、デバイス情報処理モジュール901による、ログデータアップロードの通知に対する処理手順を示すフローチャートである。

【0161】

ログデータをアップロードする通知を受けると、共通情報処理モジュール1201を起動し（ステップS1601）、ログデータを含むMIFファイルの送付要求をデバイス監視モジュール203aに発行する（ステップS1602）。

【0162】

その要求への応答であるMIFファイルを受信し（ステップS1603）、それをインベントリデータベース109へ格納する（ステップS1604）。MIFファイルの削除要求をデバイス監視サーバ203aに対して発行し（ステップS1605）、それらの処理が終了すると処理終了の旨をバックエンドに通知する（ステップS1606）。

【0163】

<デバイス監視サーバによる処理手順>

図17は、拠点プラグイン203bにおいて、プラグインに対して発行されたメッセージあるいはイベントに対する処理手順を示すフローチャートである。なお、センタサーバ110から拠点プラグイン203bにあって発行されたメッセージは、監視クライアント203dにより所定の領域に格納されるために、拠点プラグイン203bはそれを常時あるいは一定時間おきに監視し続けている。

## 【0164】

メッセージがあると、それがデバイス監視サーバ203aからのメッセージであるか判定し（ステップS1701）、そうであれば、メッセージを解析して（ステップS1702）、警告や閾値越えであれば、ログデータをMIFファイルとして書き出し、PC監視クライアント203dを介して、ログファイルのアップロードを行う旨、センタサーバ110にあててイベントを発行する（ステップS1705）。

## 【0165】

警告や閾値越えではない場合には、エラーであるか判定し（ステップS1706）、エラーであれば障害イベントを示すメッセージを作成してステップS1705へ分岐する。（ステップS1707）。

## 【0166】

デバイス監視サーバ203aからのメッセージでない場合には、センタサーバ110からのメッセージであると判定して、PC監視クライアント203dにより書き出された所定の領域を読み出し（ステップS1708）、そのデータを解析して内容に応じた処理を遂行する。この解析した内容に応じた処理の詳細が図18に示されている。

## 【0167】

図18は、拠点プラグイン203bによる、センタサーバ110から受信したメッセージ維持に応じた処理の手順を示すフローチャートである。

## 【0168】

まず、それがダウンロードデータであるか判定し（ステップS1801）、ダウンロードデータであれば、デバイス監視サーバ203aに対してダウンロードデータの受信を通知し（ステップS1802）そのデータを渡す（ステップS1

803)。そして、渡し終えたデータを削除し（ステップS1804）、センタサーバにあててダウンロード完了イベントを発行する（ステップS1805）。

【0169】

ダウンロードデータでない場合には、デバイス情報の収集要求であるか判定し（ステップS1806）、そうであれば、デバイス監視サーバ203aに対してデバイスじょうほうの収集を要求する（ステップS1807）。

【0170】

それに応じてデバイス監視サーバ203aからデバイス情報を受信すると（ステップS1808）、それをMIFファイルとして格納し（ステップS1809）、デバイス情報を収集した旨のメッセージをセンタサーバ110にあてて発行する。

【0171】

#### <PC監視クライアントによる処理手順>

図19は、PC監視クライアントがメッセージを受信した場合の処理手順を示すフローチャートである。

【0172】

図19において、受信データの宛先がどこであるか判定し（ステップS1901）、PC・サーバといった汎用コンピュータにあてたデータであれば、指定されたプロセスへとそのデータを渡し（ステップS1902）、拠点プラグインであれば、前述した所定の領域へとデータを書き込む。

【0173】

以上のように、本実施形態のシステムでは、汎用コンピュータ用の監視システムを用いて、監視対象の汎用コンピュータと同じ被管理サイトに設置された周辺機器をも管理することができる。これにより、管理サイトにおいては、汎用コンピュータと周辺機器とを同様な方法で一元的に監視することができる。さらに、周辺機器に関する情報の収集や、パラメータの設定等を、その監視システムを通して管理サイト側から行える。また、被管理サイト側から、ログを管理サイトに対して送信することができる。

【0174】

さらに、汎用コンピュータ用の監視システムに対して、周辺機器を管理するために付加するモジュールは、すべてソフトウェア的に実現できるために、そのためのハードウェアを必要とせず、設置面積や機器の費用、維持作業等、ハードウェア的な規模の増大を防止できる。

## 【0175】

また、本発明は汎用コンピュータ（PC・サーバ系）の管理ソフトにデバイス系の管理情報を適合させるものに限定されるものではなく、その逆、即ち周辺機器（デバイス系）の管理ソフトにPC・サーバ系の管理情報を適合させるものにすることも可能である。例えば、図9中のデバイス系201とPC・サーバ系202とを、デバイス監視サーバ203aとPC監視クライアントモジュール203dとを、それぞれ入れ替え、MIFファイル203eをデバイス固有のファイル形式にし、拠点プラグイン203bにはPC・サーバ系のフォーマット形式をデバイス系のフォーマット形式に変換させる機能を持たせ、また、センタサーバにデバイス系の処理をさせ、デバイス処理モジュール901にPC・サーバ系の情報を処理させデバイスセンタにイベントを発行させるなどの形態が考えられる。

## 【0176】

## ＜センターコール＞

上記で説明した第1の遠隔サイト管理システム或いは第2の遠隔サイト管理システムにおいて、被管理サイトの顧客が管理サイトに電話をしたときに、管理サイトで使用されるアプリケーションシステムについて説明する。上記で説明した遠隔管理サイト管理システムでは、オフィス内の機器で障害が発生したときには、通常、その旨の通知がデバイス監視サーバ203aからデバイスセンタサーバへ送信される。

## 【0177】

しかし、この通知とは別に、被管理サイトの顧客が自ら異常を察知したとき、ただし、具体的に障害を特定できなかったときには、顧客が直接管理サイトに電話で通知（センターコール）する場合がある。この場合、管理サイトのスタッフは顧客に対して或いは障害に対して適切な対応をとらなければならない、そのため

に、このアプリケーションシステム（センターコール用アプリケーションシステム）を利用する。

【0178】

＜センターコール用アプリケーションシステム＞

図20～図22は、センターコール用アプリケーションシステムが行なう処理を示すフローチャートである。まず、スタッフが顧客の電話番号を入力する入力画面を表示し、電話番号の入力を待つ。そして、電話番号が入力されると、その電話番号をキーにして、ユーザ情報をインベントリデータベースから取得する（ステップS2001）。そして、そのユーザ情報を表示画面に表示する（ステップS2002）。

【0179】

図23は、ユーザ表示画面の一例を示す図である。この画面では、顧客の名前、部署、連絡先が表示されている。また、機器一覧2302には、その顧客先に設置されている機器が一覧表示される。図では、選択ボタン2301で“ALL”が選択されているため、デバイス系機器、PC・サーバ系機器が全て表示されている。ここで、“DEVICE”が選択されるとデバイス系機器だけが表示され、“PC”が選択されるとPC系機器が一覧表示される。

【0180】

従って、スタッフは、顧客からの情報に基づいて、デバイス系の障害が発生していると判断すると、“DEVICE”を選択する。また、PC・ネットワーク系の障害が発生していると判断すると、“PC”を選択する。そして、いれずれとも食んだできなかった場合には、“ALL”を選択する。

【0181】

一方、センターコール用アプリケーションシステムは、ユーザが“DEVICE”、“PC”、“ALL”のいずれを選択したか判断する。まず、“DEVICE”が選択ボタンにより選択されているか否かに応じて、デバイス系の障害が発生したか否かを判定する（ステップS2003）。デバイス系の障害発生していると判定した場合には、ステップS2100に進む。そうでなければ、ステップS2004に進み、“PC”が選択ボタンにより選択されているか否かに応じ

て、PC・ネットワーク系の障害が発生したか否かを判定する（ステップS2004）。PC・ネットワーク系の障害発生していると判定した場合には、ステップS2200に進み、そうでなければ、ステップS2005に進む。

## 【0182】

## ＜デバイス系の障害＞

ステップS2003において、デバイス系の障害が発生していると判定した場合には、ステップS2010に進み、デバイス監視サーバに診断を行なわせるように要求を出す（ステップS2010）。具体的には、情報収集を指示するメッセージをデバイスセンタサーバへ送信する。すると、デバイスセンタサーバは、図5の処理によって、情報収集要求をデバイス監視サーバに発行する。次に、デバイス監視サーバからの情報をデバイスセンタサーバを介して受信する（ステップS2011）。

## 【0183】

そして、障害の内容が、デバイス監視サーバによって切り分け可であるか否かを判定する（ステップS2012）。切り分け可である場合とは、デバイス監視サーバで障害が検出できた場合（例えば、受信した情報に障害イベントが含まれている場合）などである。切り分けが不可の場合には、修理A（図21）を行なう。

## 【0184】

切り分けが可の場合には、更に、その障害が被管理サイトで復旧可であるか否かを判定する（ステップS2013）。被管理サイトで復旧が不可の場合には、修理B（図22）を行なう。復旧が可の場合には、障害の内容がスタッフに分かるように表示する。例えば、図24の表示画面では、レーザビームプリンタである“LB1810”が電源OFFであることを点滅表示する。すると、スタッフはその表示を見て、顧客にアドバイスする。

## 【0185】

## ＜PC・ネットワーク系の障害＞

ステップS2004において、PC・ネットワーク系の障害が発生していると判定した場合には、ステップS2020に進み、PC監視クライアントに診断を

行なわせるように要求を出す（ステップS2020）。具体的には、情報収集を指示するメッセージをセンタサーバへ送信する。すると、センタサーバは、情報収集要求をPC監視クライアントに発行する。次に、PC監視クライアントからの情報をセンタサーバを介して受信する（ステップS2021）。

## 【0186】

そして、障害の内容が、PC監視クライアントによって切り分け可であるか否かを判定する（ステップS2022）。切り分け可である場合とは、PC監視クライアントで障害が検出できた場合（例えば、受信した情報に障害イベントが含まれている場合）などである。切り分けが不可の場合には、修理A（図21）を行なう。

## 【0187】

切り分けが可の場合には、更に、その障害が被管理サイトで復旧可であるか否かを判定する（ステップS2023）。被管理サイトで復旧が不可の場合には、修理B（図22）を行なう。復旧が可の場合には、障害の内容がスタッフに分かるように表示する。例えば、図25の表示画面では、ネットワークルータである“Router-01”が電源OFFであることを点滅表示する。すると、スタッフはその表示を見て、顧客にアドバイスする。

## 【0188】

## ＜デバイス系又はPC・ネットワーク系の障害の判定＞

ステップS2003及びS2004において、デバイス系とPC・ネットワーク系とのいずれの障害とも判定できなかった場合には、具体的には、スタッフが、選択ボタン2301において、“ALL”を選択した場合には、PC監視クライアントとデバイス監視サーバとのそれぞれに診断を行なわせるように要求を出す（ステップS2005）。具体的には、情報収集を指示するメッセージをデバイスセンタサーバやセンタサーバへ送信する。すると、センタサーバは、情報収集要求をPC監視クライアントに発行する。また、デバイスセンタサーバは、情報収集要求をデバイス監視サーバへ発行する。次に、デバイス監視サーバとPC監視クライアントからの情報をデバイスセンタサーバとセンタサーバを介して受信する（ステップS2006）。

## 【0189】

そして、障害の内容が、デバイス監視サーバとPC監視クライアントとの組み合わせによって切り分け可であるか否かを判定する（ステップS2007）。切り分け可である場合とは、デバイス監視サーバやPC監視クライアントで障害が検出できた場合（例えば、受信した情報に障害イベントが含まれている場合）などである。切り分けが不可の場合には、修理A（図21）を行なう。

## 【0190】

切り分けが可の場合には、更に、その障害が被管理サイトで復旧可であるか否かを判定する（ステップS2008）。被管理サイトで復旧が不可の場合には、修理B（図22）を行なう。復旧が可の場合には、障害の内容がスタッフに分かるように表示する。すると、スタッフはその表示を見て、顧客にアドバイスする。

## 【0191】

図26は、ステップS2007の判定において、切り分けが可の場合の事例である。コール内容は、スタッフが顧客から電話で聞いた内容である。監視結果は、PC監視クライアント及びデバイス監視サーバから送られてきた情報の内容である。

## 【0192】

まず、1番目の事例では、PC1からプリンタ1にプリントの指示が出されたが、プリント処理が行なわれなかった。そこで、デバイス監視サーバとPC監視クライアントに診断を行なわせた結果、PC1及びプリンタ1は正常であった。ただし、プリントサーバの役割をしているPCのハードディスクの空き容量が200Kバイトまで減っていた。そこで、プリントサーバのハードディスク容量が少なく、プリントデータが正しく格納されない（スプールされない）と判定し、プリントサーバのハードディスクの空き容量を確保するよう対処すると判断した。

## 【0193】

また、2番目の事例では、新しくPC2をセットアップして、プリンタの設定を行なったが、PC2からプリンタ2は見えるが、プリンタ3は見えない。そこ



で、デバイス監視サーバとPC監視クライアントに診断を行なわせた結果、ルータ1、プリンタ2、プリンタ3は正常であった。ただし、PC2からの反応がなかった。そこで、新規PC2は、デフォルトゲートウェイの設定が正しく行なわれずに、セグメントを越えての通信ができなかったと判定し、PC2におけるデフォルトゲートウェイにルータ1のIPアドレスを設定するよう対処すると判断した。

## 【0194】

3番目の事例では、PC3からプリンタ4にプリント指示を出したが、プリンタ処理が行なわれなかった。そこで、デバイス監視サーバとPC監視クライアントに診断を行なわせた結果、PC3は正常であったが、プリンタ4でソータの接続不良が検出された。そこで、プリンタ4のソータが正しく接続されていないと判定し、ソータを正しく接続するよう対処すると判断した。

## 【0195】

## &lt;修理A&gt;

図21は、センターコール用アプリケーションシステムが、修理Aを行なう場合の処理を示すフローチャートである。修理Aは、ステップS2012、S2022、S2007で、デバイス管理サーバやPC監視クライアントによる切り分けができないと判定された場合に実行される。

## 【0196】

修理Aでは、障害の内容が切り分けされなかったために、まず、サービスマンを被管理サイトへ向かわせる（ステップS2101）。具体的には、サービスマンが持っている情報携帯端末、例えば、ノートパソコンや携帯電話にディスパッチ情報を送信し、図27のような表示画面を情報携帯端末に表示させる。

## 【0197】

図27は、サービスマンの情報携帯端末に表示されるディスパッチ画面の一例である。ここでは、まず、向い先の顧客情報（顧客名や電話番号）を表示する。そして、現地に向えるかどうか、向える場合には何分で到着できるかをサービスマンに入力させ、その内容を受信する。

## 【0198】

次に、顧客先に向けたサービスマンからの障害報告を待ち、それを受信する（ステップS2102）。この障害報告は、被管理サイトのデバイス監視サーバやPC監視クライアントでサービスマンによって入力され、それをデバイスセンタサーバやセンタサーバを介して受信する。その障害報告に基づいて、障害が自社で対処可能であるか否かを判定する（ステップS2102）。

#### 【0199】

自社で対応可能な場合には、そのままサービスマンが復旧作業を行なうので、復旧が確認されるのを待つ（ステップS2104）。デバイス監視サーバ或いはPC監視クライアントから受信された情報により、復旧が確認されたのち処理を終了する。

#### 【0200】

自社で対応不可能な場合には、協力会社へ作業依頼を出す（ステップS2105）。自社が主にデバイス系の機器を扱っていて、PC系の障害が発生した場合には、その復旧作業（メンテナンスサービス）を協力会社をお願いするためである。ここで、図28に示すような依頼書が電子メールで協力会社に送られるものとする。この依頼書には、ユーザ情報の他、障害が発生している機器の機器情報も盛り込まれる。障害が発生している機器の特定は、ステップS2102における障害報告に基づいて行なわれる。ステップS2105では、依頼書のテンプレートとなるファイルをまず読み出し、そこに、ステップS2001で引き出したユーザ情報を埋め込む。次に、障害内容をもとに機器を特定し、その機器に関する機器情報を埋め込む。更に、受信された障害内容をコメントとして所定の欄に埋め込む。そのファイルを電子メールに添付して協力会社に送信する。

#### 【0201】

協力会社のサービスマンがメンテナンス作業を行なうので、それが終了し、復旧が確認されるのを待つ（ステップS2106）。更に、協力会社から、図29のような作業レポートを電子メールで受信する（ステップS2106）。

#### 【0202】

図29は、協力会社からの作業レポートの一例を示す図である。このレポートには、作業を行なった時間、メンテナンス対象機器の機種名とシリアル番号、障

害の原因、処置内容が示されている。また、メンテナンス代行に対する料金を、のちにこの協力会社に支払うために、作業レポートの内容に関する情報を依頼履歴としてデータベースに格納しておく（ステップS2108）。

#### 【0203】

##### <修理B>

図22は、センターコール用アプリケーションシステムが、修理Bを行なう場合の処理を示すフローチャートである。修理Bは、ステップS2013、S2023、S2008で、被管理サイトでの復旧ができないと判定された場合に実行される。

#### 【0204】

修理Bでは、既に障害内容が把握されているので、まず、デバイス監視サーバやPC監視クライアントからの情報をもとに障害レポートを作成する（ステップS2201）。図30は、障害レポートの一例を示す図である。障害レポートには、障害が発生した時刻、障害が発生した機器の機種名及びシリアル番号、障害の原因、障害への対処方法が示されている。

#### 【0205】

次に、障害が自社で対処可能であるかを判定する（ステップS2202）。自社で対処可能である場合には、サービスマンを被管理サイトへ向わせる（ステップS2103）。具体的には、図21のステップS2101と同様にである。更に、障害レポートを電子メールに添付してサービスマンの情報携帯端末に送信し、必要な部品の手配処理を行なう（ステップS2204）。そして、顧客先に向ったサービスマンが復旧作業を行ない、復旧が確認されるのを待つ（ステップS2205）。デバイス監視サーバ或いはPC監視クライアントから受信された情報により、復旧が確認されたのち処理を終了する。

#### 【0206】

自社で対応不可能な場合には、協力会社へ作業依頼を出す（ステップS2206）。ここでは、図21のステップS2105と同様に、依頼書が電子メールで協力会社へ送られる。それとともに、障害レポートも電子メールで協力会社へ送られる。協力会社のサービスマンがメンテナンス作業を行なうので、それが終了

し、復旧が確認されるのを待つ（ステップS2207）。更に、協力会社から、図29のような作業レポートを電子メールで受信する（ステップS2208）。メンテナンス代行に対する料金を、のちにこの協力会社に支払うために、作業レポートの内容に関する情報を依頼履歴としてデータベースに格納しておく（ステップS2209）。

#### 【0207】

##### <その他の実施の形態>

なお、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成される。

#### 【0208】

この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードに記憶した記憶媒体は本発明を構成することになる。

#### 【0209】

また、デバイス情報データは、画像処理装置及び画像データ展開装置に内蔵されているHDD、外部接続されている記憶媒体、画像データ展開装置からアクセス可能なサーバ等に保持されていても構わない。さらに、デバイス情報データはユーザが任意に設定したものを使用することが可能であっても構わない。

#### 【0210】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、DVD-ROM、磁気テープ、不揮発性のメモリカード、ROMなどを用いることができる。

#### 【0211】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOS（オペレーティングシステム）など

が、実際の処理の一部または全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含まれる。

#### 【0212】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

#### 【0213】

本発明を上記記憶媒体に適用する場合、その記憶媒体には、先に説明した（図5乃至図7、図13乃至図19、図20乃至図22に示す）フローチャートに対応するプログラムコードが格納されることになる。

#### 【0214】

##### 【発明の効果】

本発明は、管理サイトが、オフィスにおけるPC・サーバ系の機器とデバイス系の機器との双方を一元的に管理できる。

#### 【0215】

特に、オフィスのサービス対象の機器がエラーを起こし、オフィスの顧客が保守サービス会社に電話で通知（センターコール）したときに、エラー発生に的確に対応し、スムーズにメンテナンスの手配（サービスマンの手配、他のサービス会社への代行メンテナンス依頼）を行なうことができる。

#### 【0216】

特に、エラーの内容が把握できる場合には、障害レポートを作成し、メンテナンスに向うサービスマンがその障害レポートをもとに迅速にメンテナンス作業を行なえるようにし、また、エラーの内容が把握できない場合には、まず先にサービスマンをこきよく先に向わせるようにすることで、サービスマンに、エラー発生に対して迅速に行動をとらせることができる。

#### 【0217】

また、自社がエラーに対処可能であるか否かを判定することにより、対処可能

である場合には自社のサービスマンを自動的に手配し、退社可能でない場合には協力会社に自動的にメンテナンス代行を依頼することができる。

【図面の簡単な説明】

【図 1】

被管理サイトと管理サイトの構成を示すブロック図である。

【図 2】

本遠隔サイト管理システムのソフトウェアモジュールの構成を示すブロック図である。

【図 3】

各 PC 及びサーバであるコンピュータの構成を示すブロック図である。

【図 4】

拠点システムとセンタシステムとの間で行われる、データの交換の手順を説明するためのブロック図である。

【図 5】

デバイスセンタサーバにおけるメッセージ受信時の処理手順を示すフローチャートである。

【図 6】

デバイス監視サーバ 2 0 3 a において発生したイベントに対する処理手順を示すフローチャートである。

【図 7】

デバイス監視サーバ 2 0 3 a が、デバイスセンタサーバ 2 1 0 から受信したメッセージを受信する手順を示すフローチャートである。

【図 8】

デバイスセンタサーバ 2 1 0 とデバイス監視サーバ 2 0 3 a との間で交換されるメッセージフォーマットの一例を示す図である。

【図 9】

本実施形態の遠隔サイト管理システムのソフトウェアモジュールの構成を示すブロック図である。

【図 1 0】

拠点システムとセンタシステムとの間で行われる、デバイスへの設定値のダウンロードの手順を説明するためのフローチャートである。

【図 1 1】

拠点システムとセンタシステムとの間で行われる、カウントデータのアップロード、すなわちデバイス情報収集の手順を説明するためのフローチャートである。

【図 1 2】

拠点システムからセンタシステムへのログデータのアップロード手順を説明するためのフローチャートである。

【図 1 3】

センタサーバ 110 におけるイベント受信時の処理手順を示すフローチャートである。

【図 1 4】

デバイス情報処理モジュール 901 による、ダウンロード終了イベントに対する処理手順を示すフローチャートである。

【図 1 5】

デバイス情報処理モジュール 901 による、デバイス情報取得（カウンタアップロード）の通知に対する処理手順を示すフローチャートである。

【図 1 6】

デバイス情報処理モジュール 901 による、ログデータアップロードの通知に対する処理手順を示すフローチャートである。

【図 1 7】

拠点プラグイン 203b において、プラグインに対して発行されたメッセージあるいはイベントに対する処理手順を示すフローチャートである。

【図 1 8】

拠点プラグイン 203b による、センタサーバ 1101 から受信したメッセージ維持に応じた処理の手順を示すフローチャートである。

【図 1 9】

PC 監視クライアントがメッセージを受信した場合の処理手順を示すフローチャートである。

ャートである。

【図 2 0】

センターコール用アプリケーションシステムが行なう処理を示すフローチャートである。

【図 2 1】

センターコール用アプリケーションシステムが、修理 A を行なう場合の処理を示すフローチャートである。

【図 2 2】

センターコール用アプリケーションシステムが、修理 B を行なう場合の処理を示すフローチャートである。

【図 2 3】

ユーザ表示画面の一例を示す図である。

【図 2 4】

復旧の指示をする表示画面の一例を示す図である。

【図 2 5】

復旧の指示をする表示画面の一例を示す図である。

【図 2 6】

切り分けが可の場合の事例を示す図である。

【図 2 7】

ディスパッチ画面の一例を示す図である。

【図 2 8】

依頼書の内容を示す図である。

【図 2 9】

作業レポートの内容を示す図である。

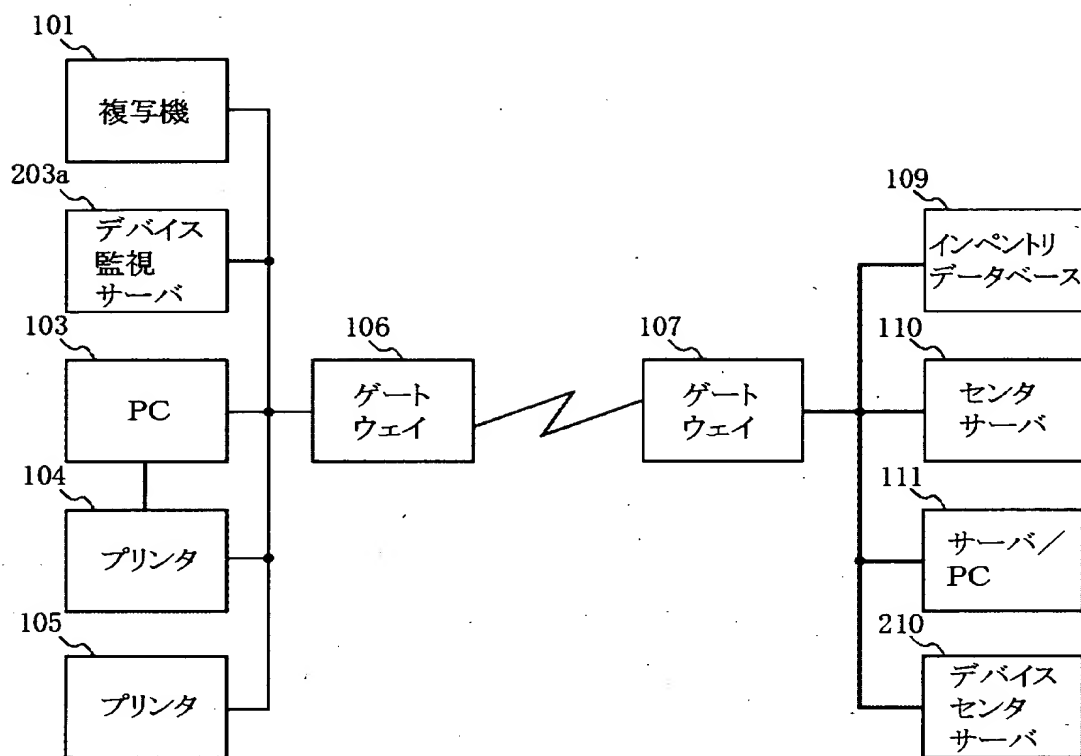
【図 3 0】

障害レポートの内容を示す図である。

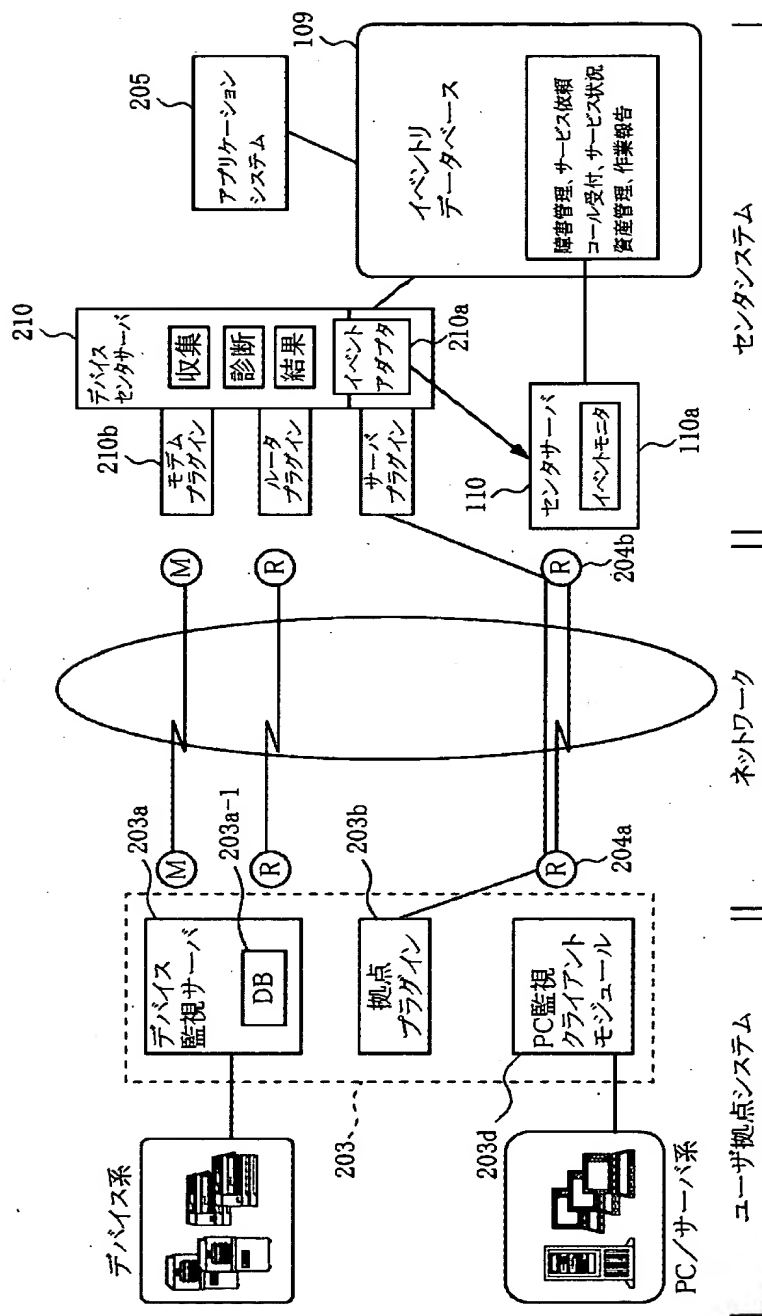


【書類名】 図面

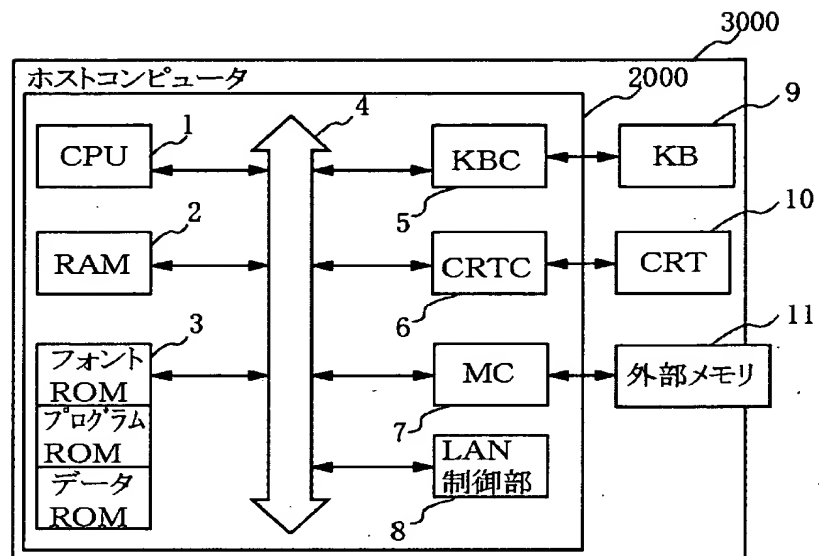
【図 1】



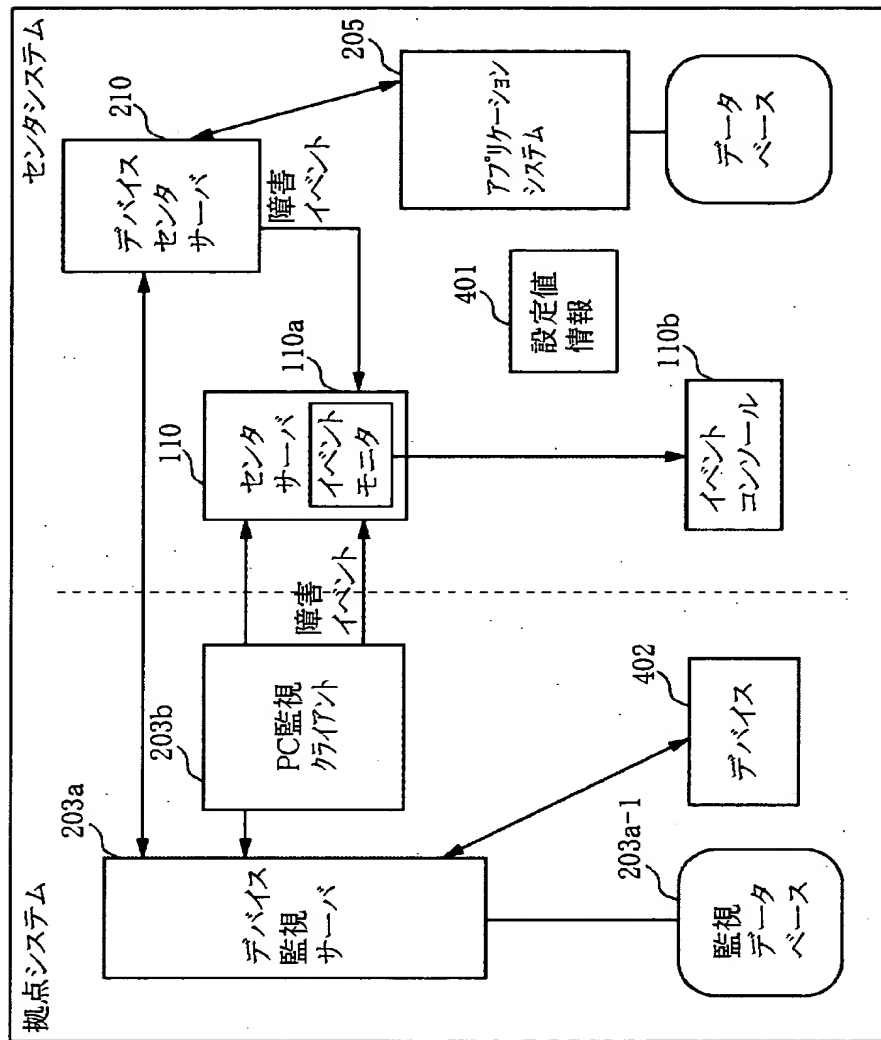
【図 2】



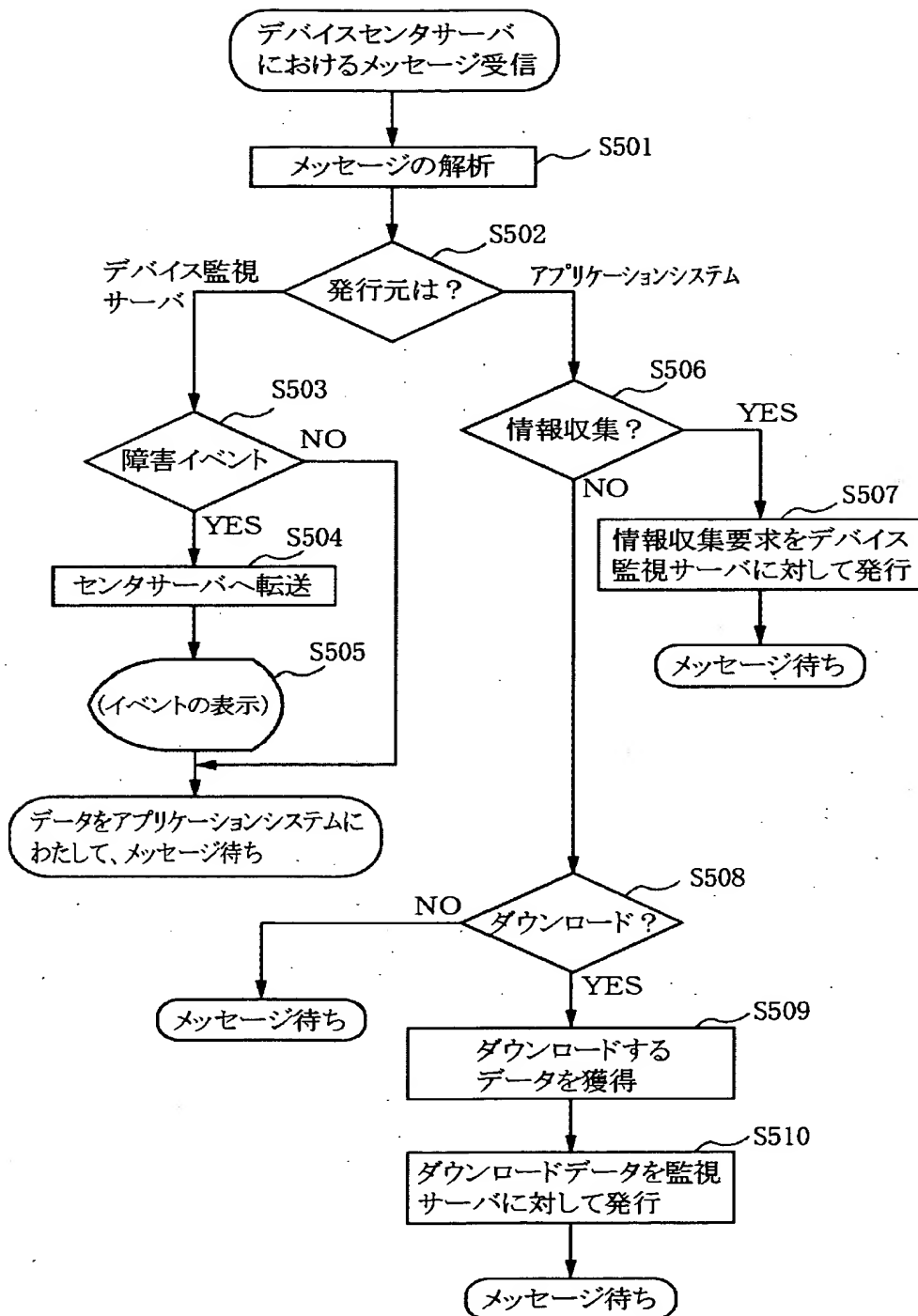
【図3】



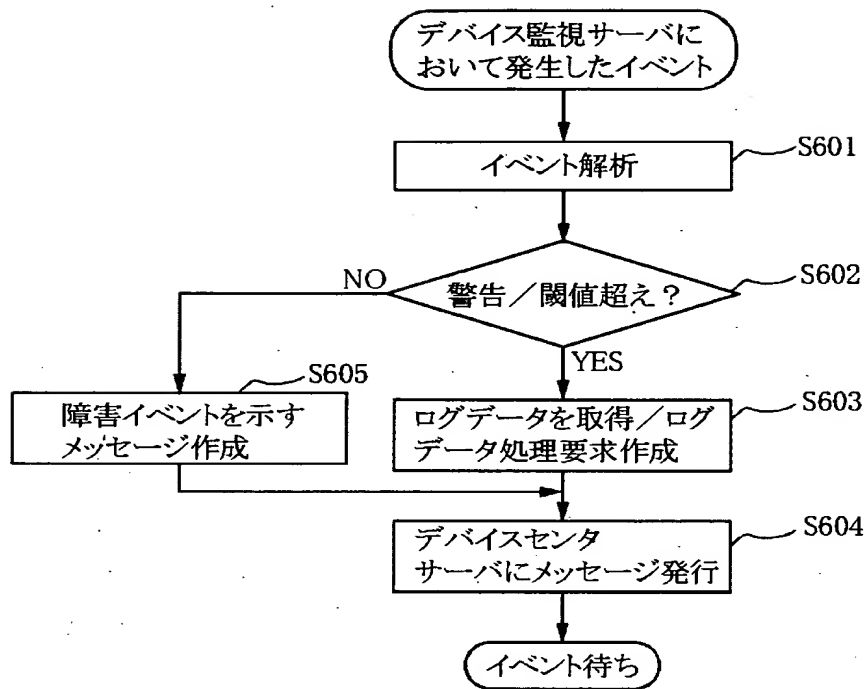
【図4】



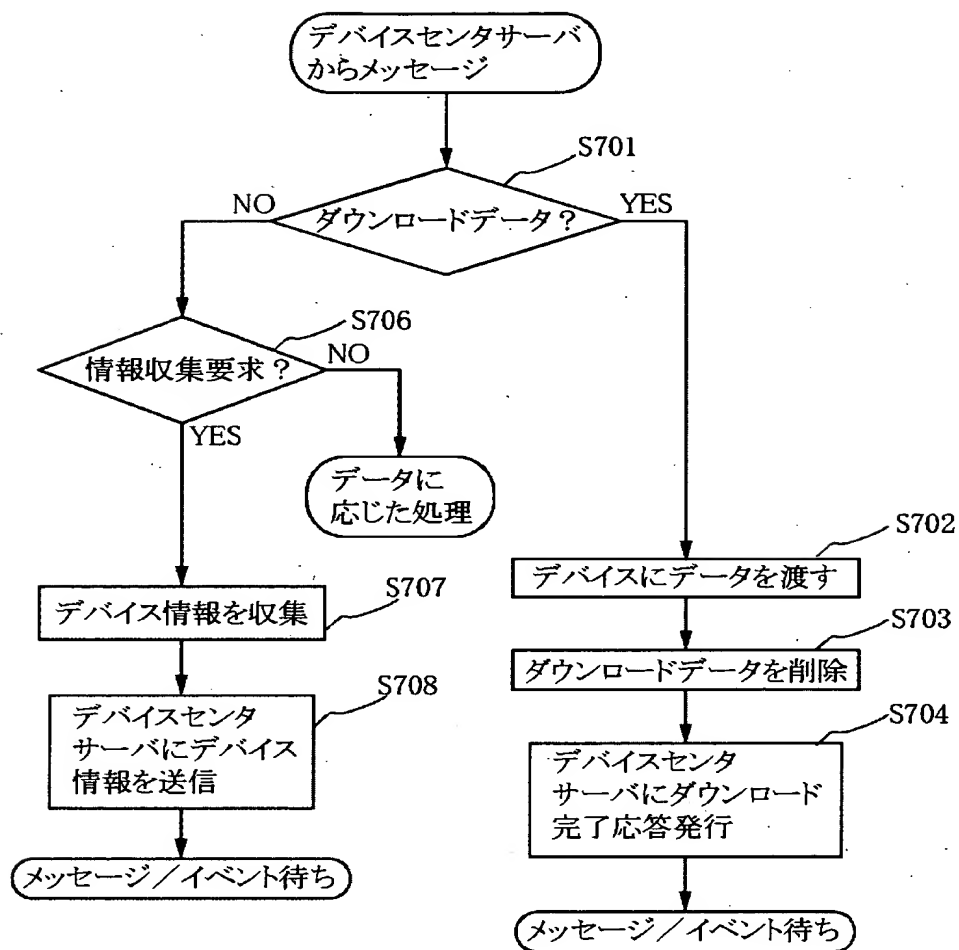
【図 5】



【図 6】



【図 7】

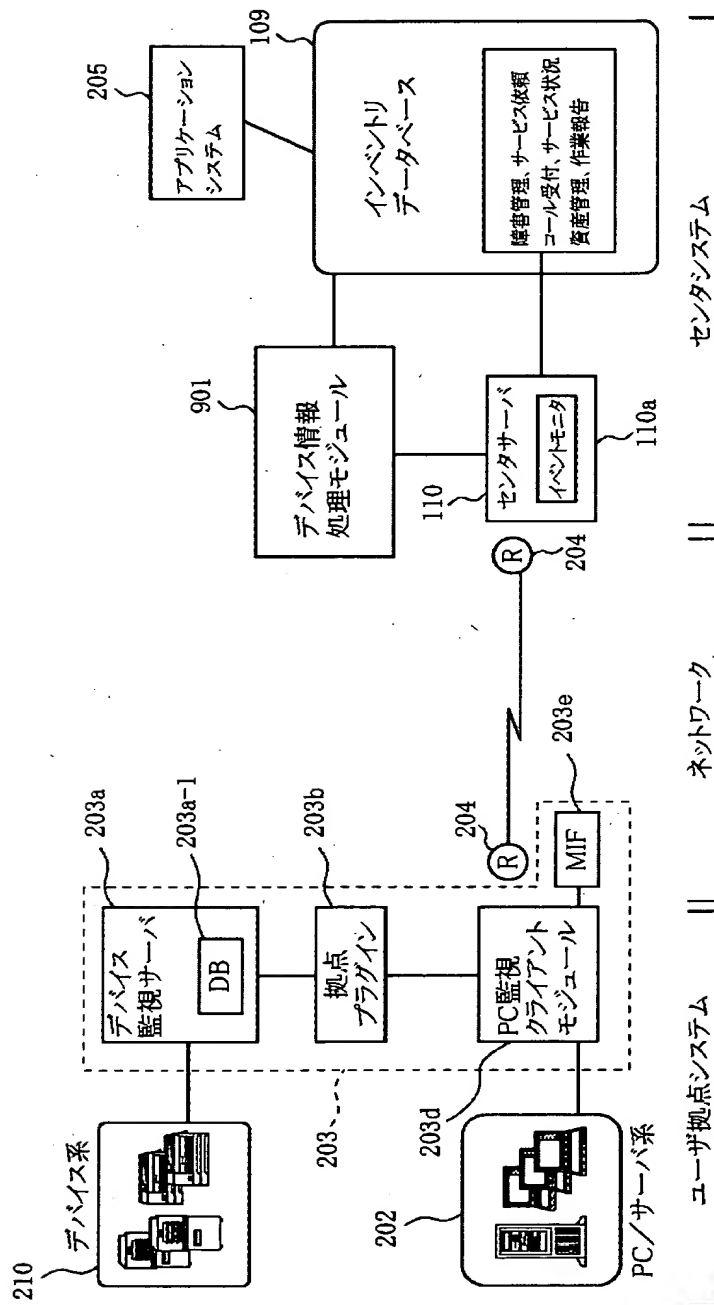


【図 8】

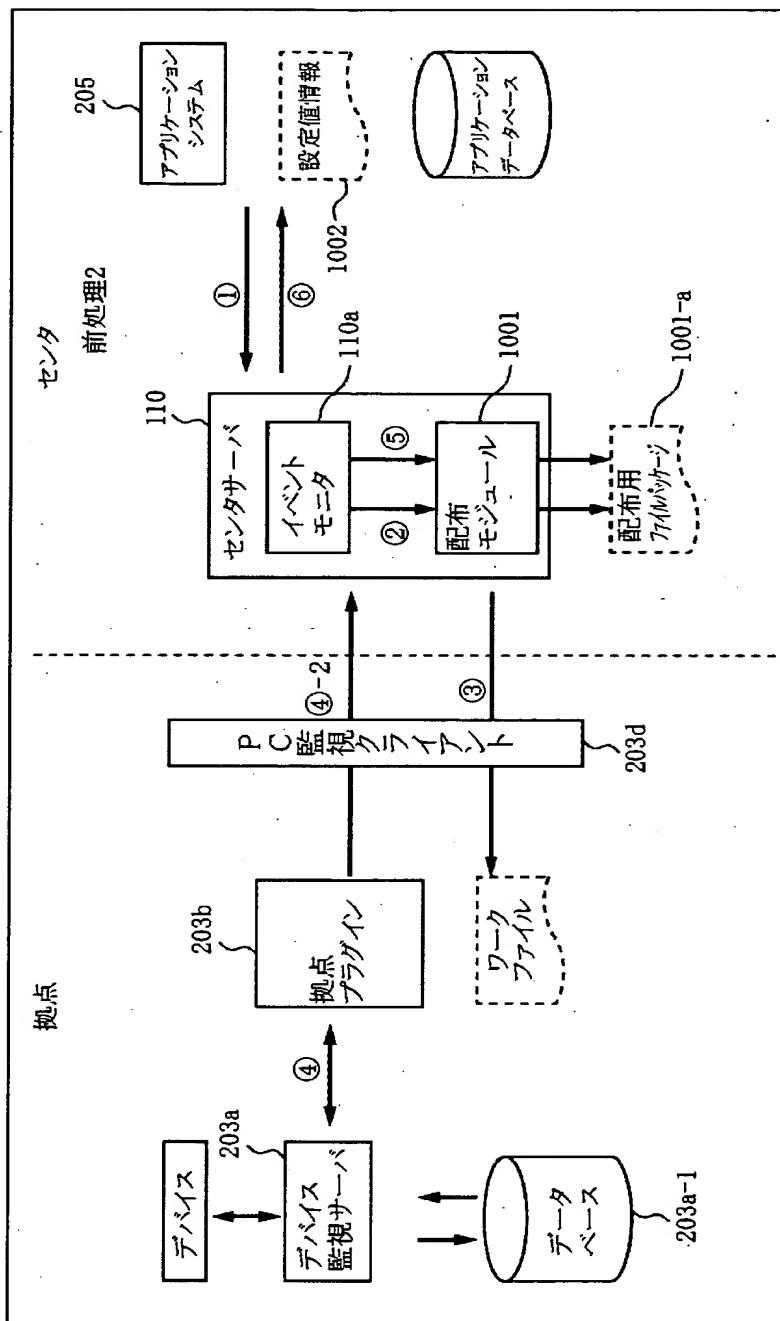
フィールド	長さ(Byte)	用途
タグ		
フラグ	1	<p>各種情報をビットで表わす。ビットの内容は以下のとおりである</p> <p>xxx..... :通信手段を示す            B'100' = TCP/IP            B'010' =ダイヤルアップ            B'001' = Eメール</p> <p>... ..x データが連続しているかを表わす            B'0' = 単純データまたは最終データ            B'1' = 連続データあり</p> <p>上記以外のビットは予備とする</p>
データ種別	1	<p>データの種別を表わす</p> <p>X'01': 認証要求データ            X'02': パラメータ設定要求データ            X'04': デバイス情報取得要求データ            X'08': イベント情報通知データ            X'10': 応答データ            X'80': 切断要求データ</p>
ジョブID	1	<p>シーケンスを区別する</p> <p>セッション中、ジョブIDは同一である必要がある</p> <p>X'00': パラメータ設定            X'01': デバイス情報取得            X'02': イベント情報通知</p>
リターン値	1	<p>データ種別が応答データ(X'10')の場合はリターン値を表わす。データ種別が切断要求データ(X'80')の場合は切断理由を表わす。データ種別が応答データ(X'10')、切断要求データ(X'80')以外の場合はX'00'をセットする</p>
データ長	4	データ長の長さをバイト数で示す(Network Byte Order)
データ	可変長	データ



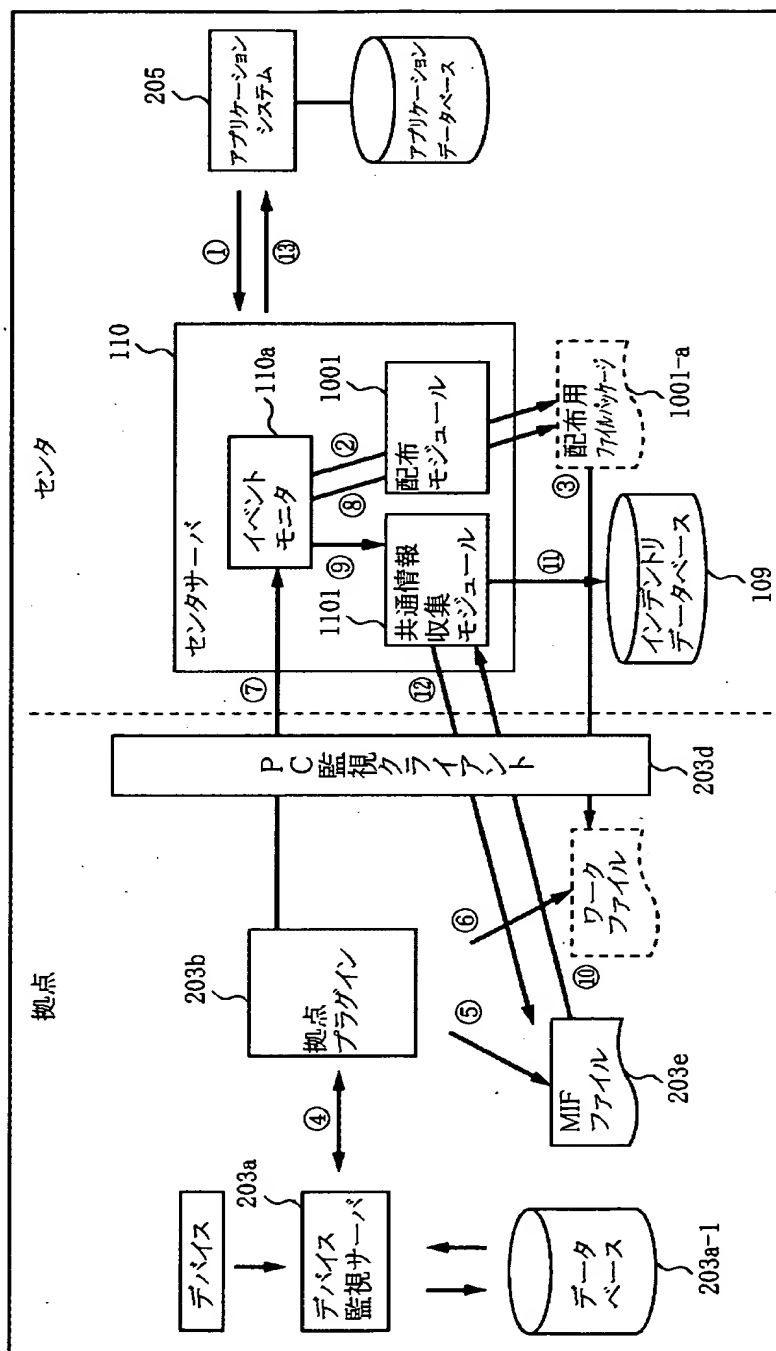
【図9】



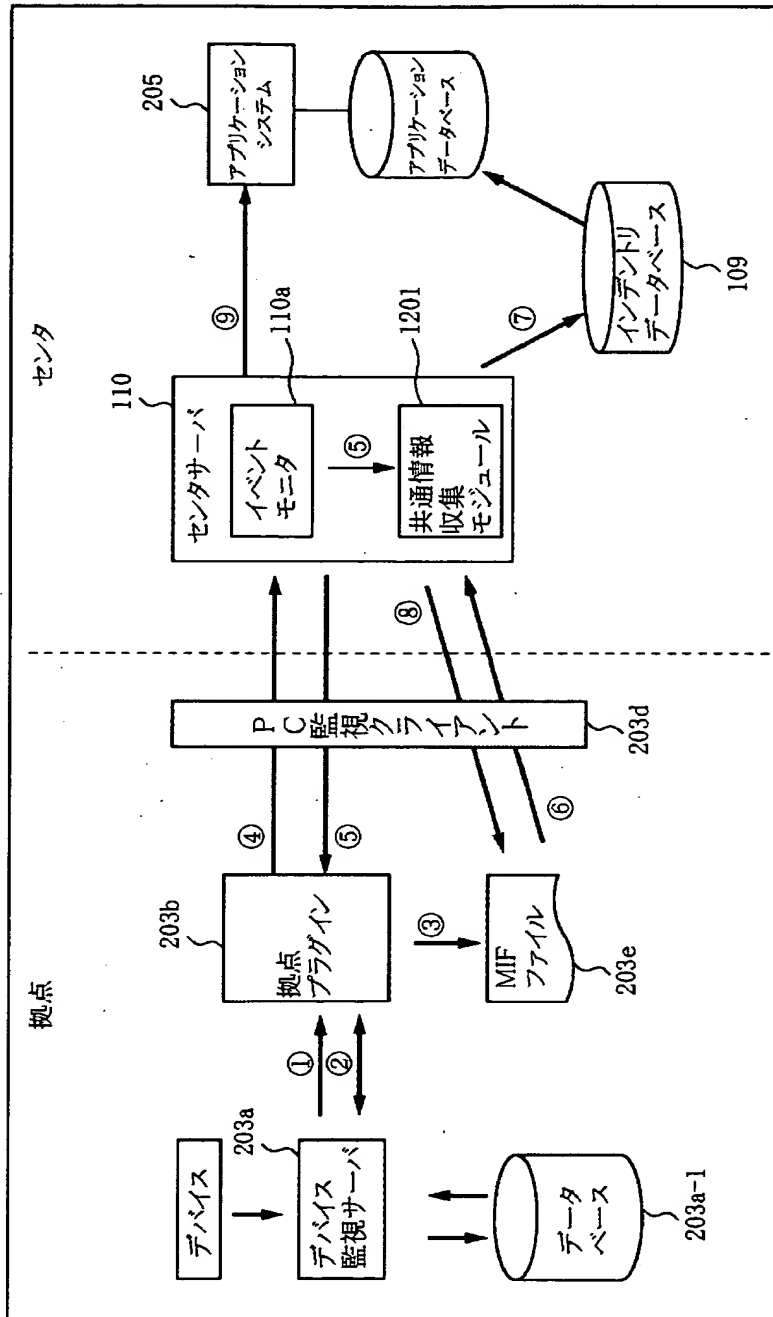
【図10】



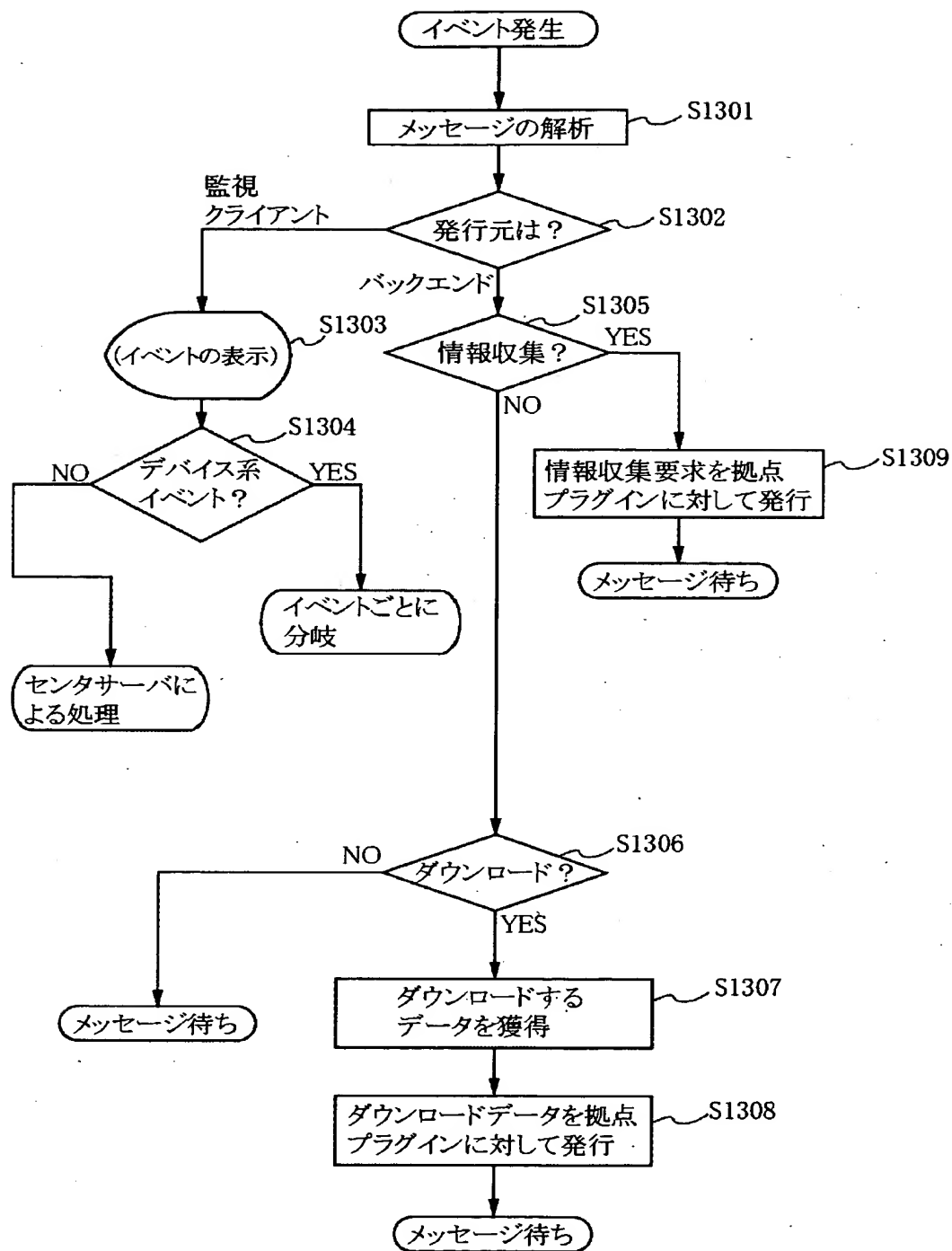
【图 1 1】



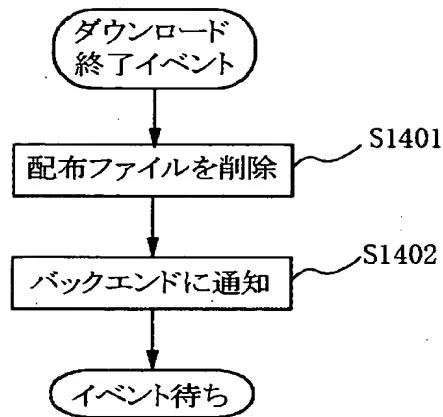
【図 12】



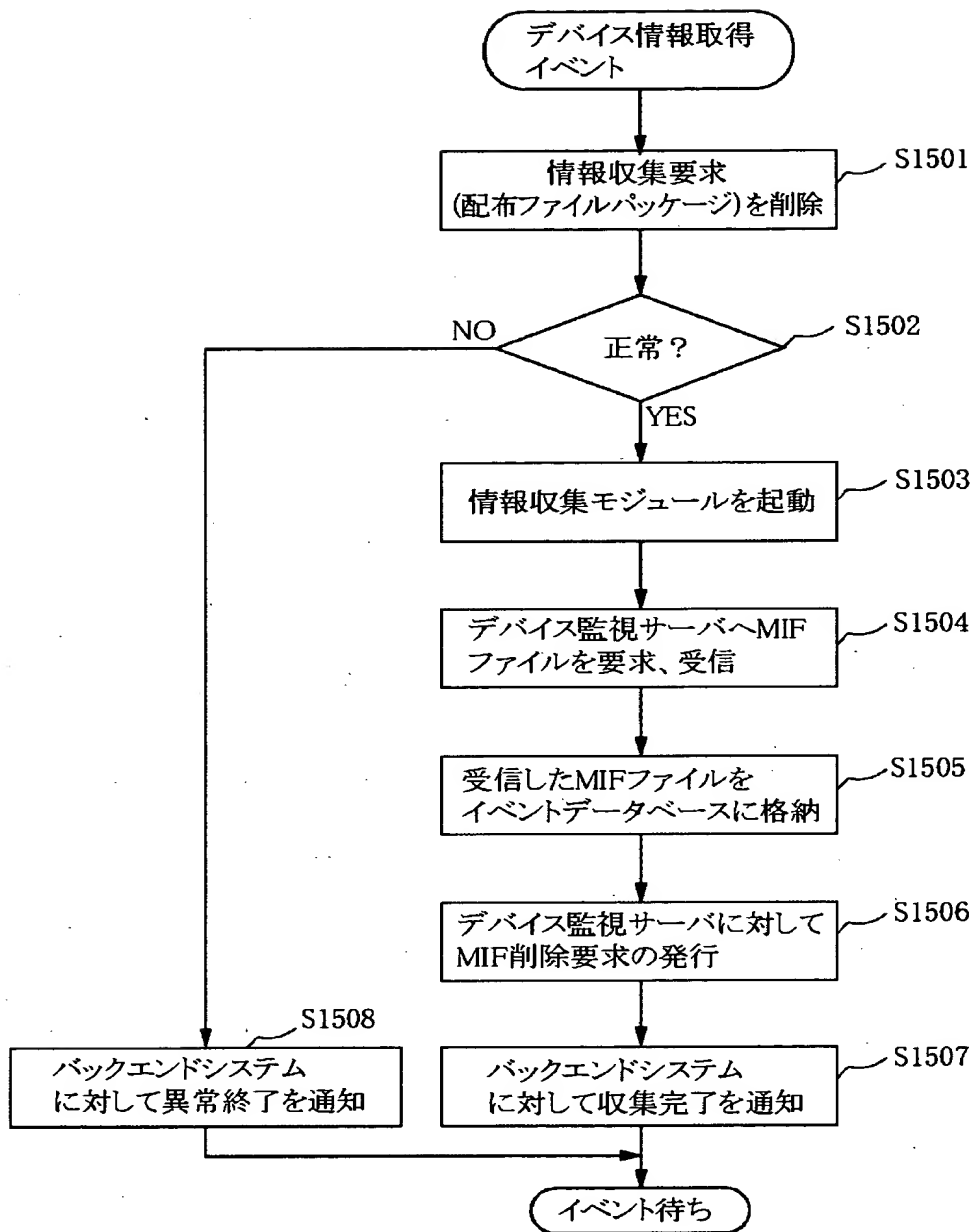
【図 1 3】



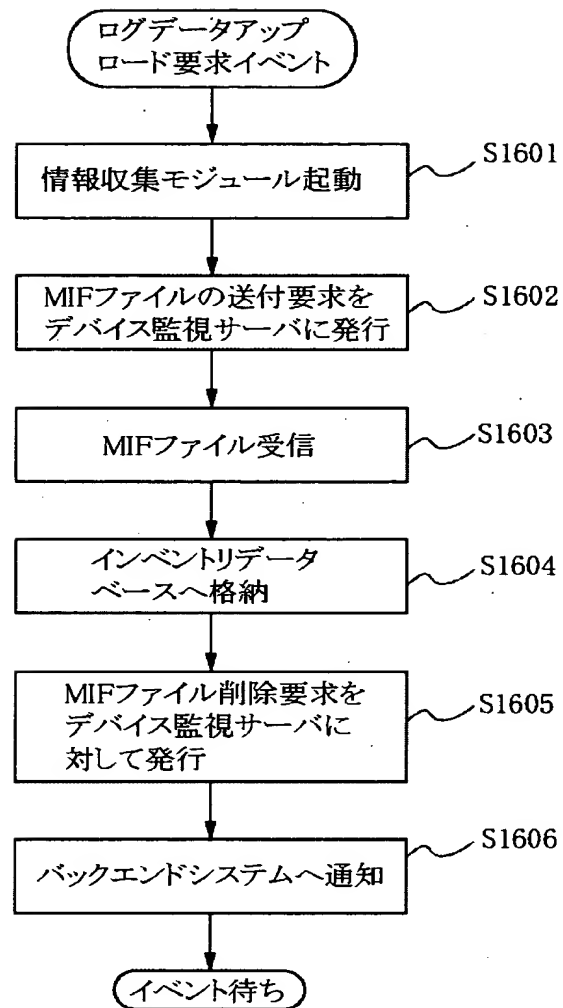
【図 1 4】



【図15】

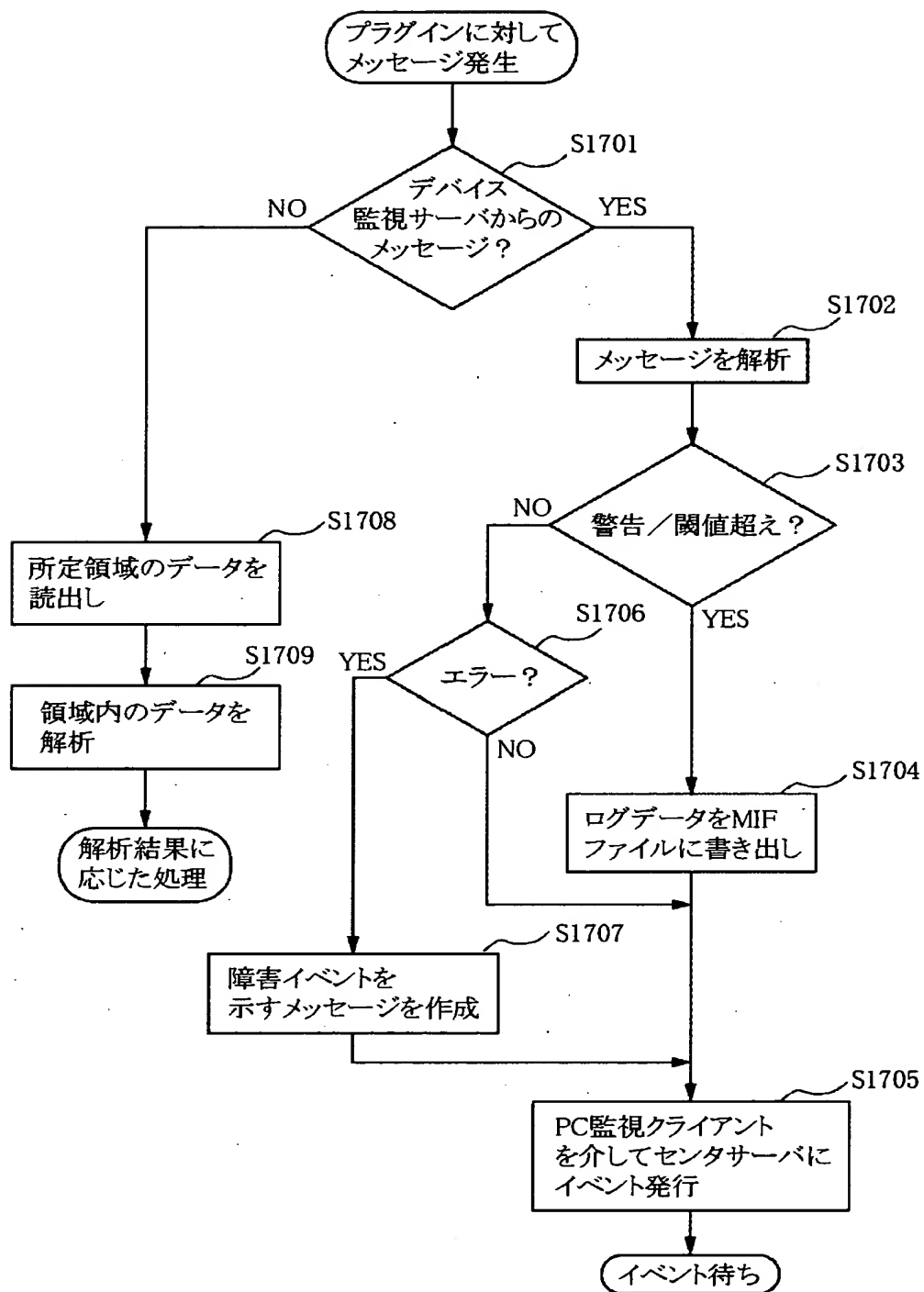


【図 1 6】

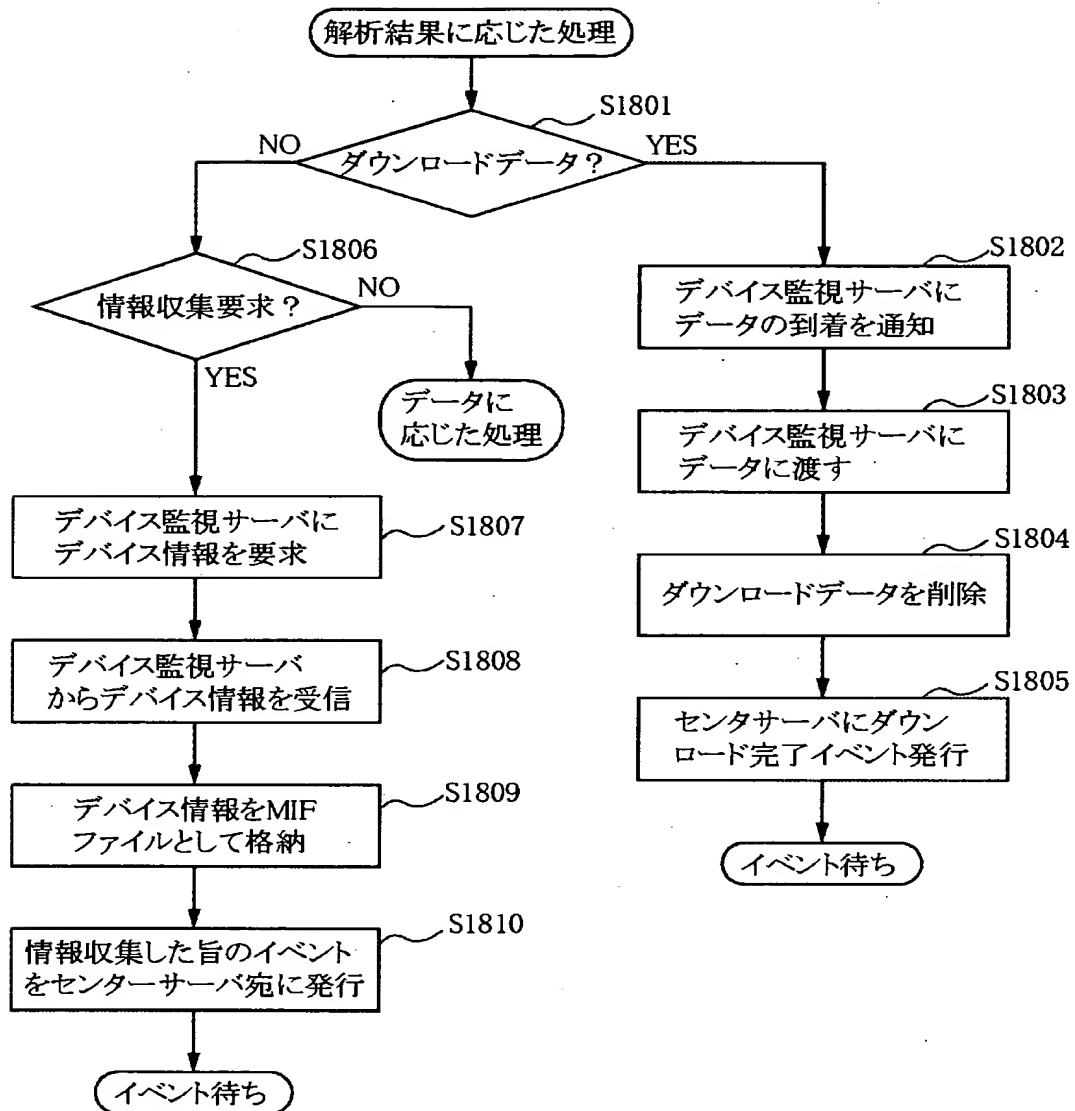




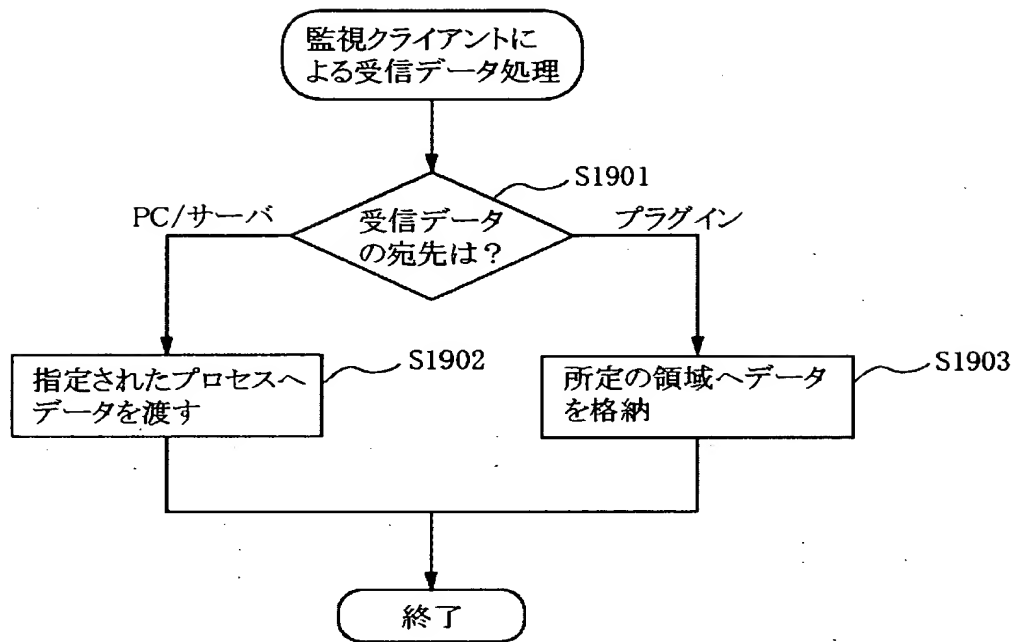
【図 17】



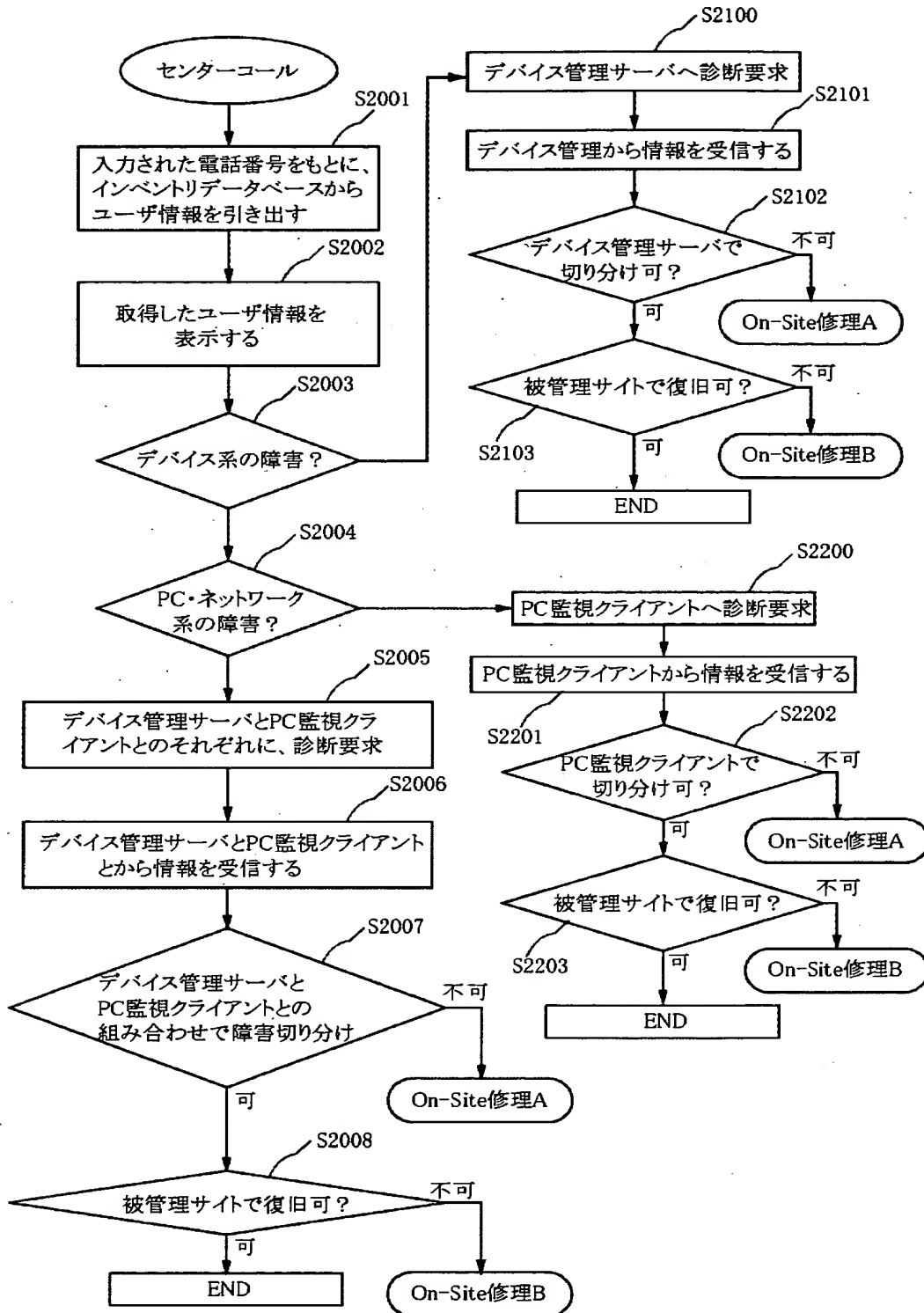
【図 1 8】



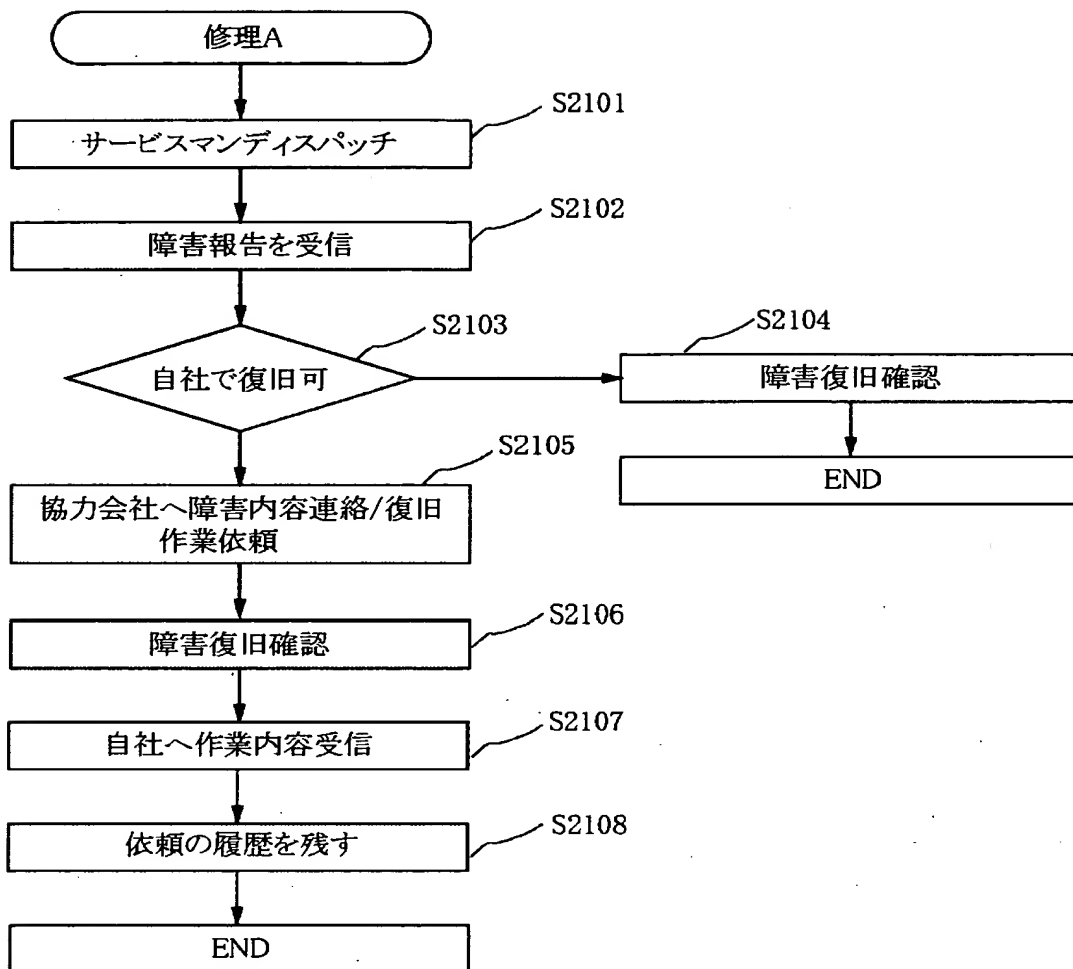
【図 1 9】



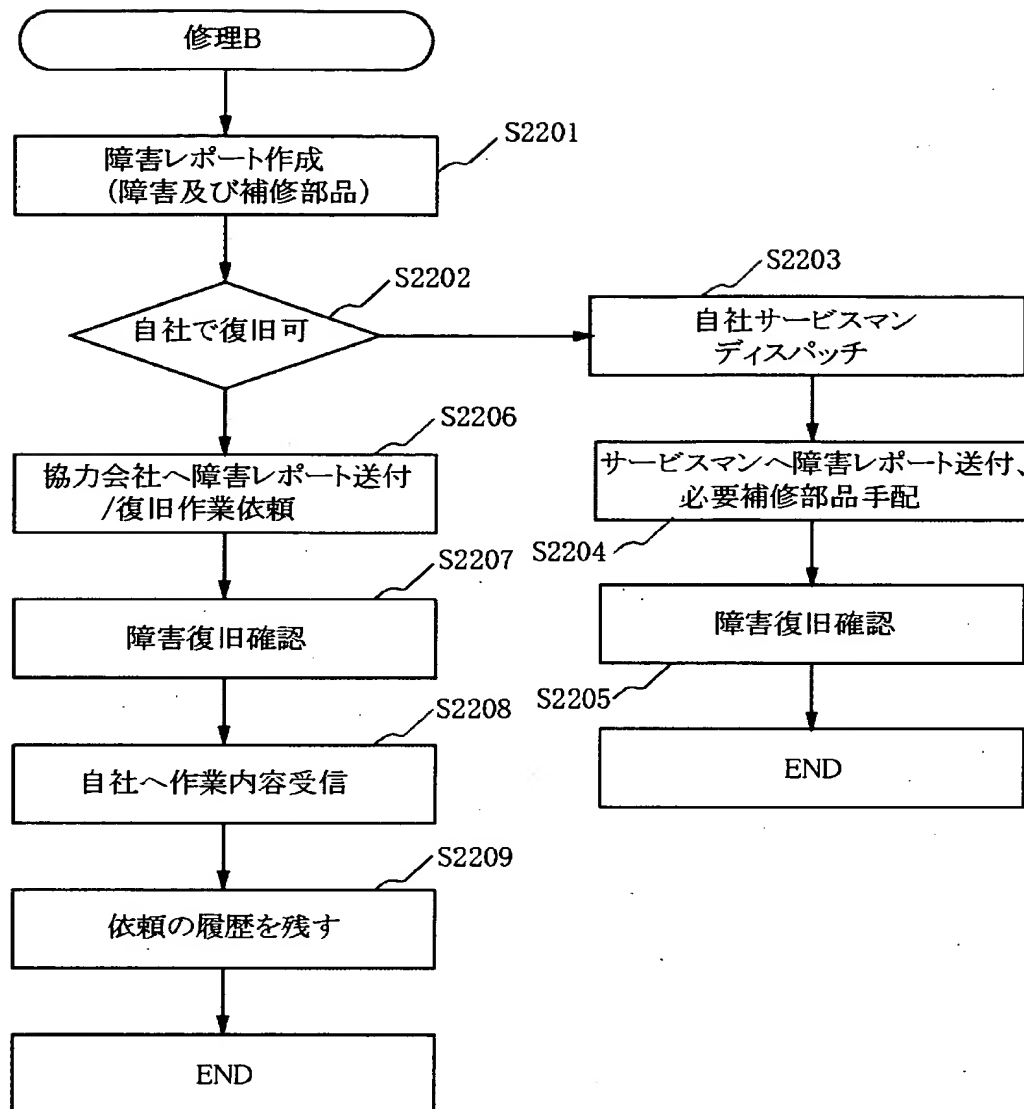
【図20】



【図 2 1】



【図 2 2】



【图 2 3】

ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(Q) ツール(T) データ(D) ウィンドウ(W) ヘルプ(H)

---

### ユーザ情報

顧客名	
部署	
連絡先(電話)	
連絡先(FAX)	
連絡先(E-mail)	

2301  
 ALL

### 機種一覧

名称	機番/シリアル番号	設置場所	ステータス
<input checked="" type="checkbox"/> IR5000	ABC12345	1F奥	
<input checked="" type="checkbox"/> LBP1810	XYZ98765	1F中央	
<input checked="" type="checkbox"/> NetFinity-01	00008514A88B	1F奥サーバー室	
<input checked="" type="checkbox"/> NetFinity-02	0000852B100A	1F奥サーバー室	
<input checked="" type="checkbox"/> Router-01	000077317A2B	1F奥サーバー室	
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

モニター  
閉じる

2302

【図 24】

[illegible]



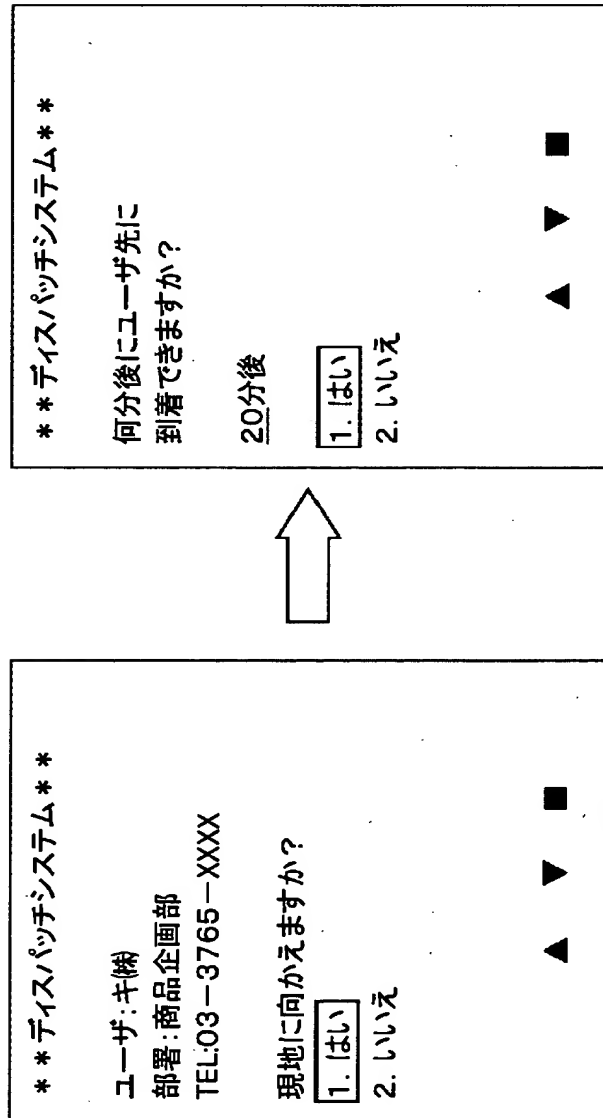
【圖 25】

[illegible]

【図 2 6】

コール内容(現象)	監視結果	原因/対処	顧客のシステム構成
PC1からプリンタ1にプリントしたが、プリントされない。 今まではプリントできていた。	<p>【PC監視クライアント】</p> <ul style="list-style-type: none"> <li>・PC1は正常。</li> <li>・プリンタ1は正常。</li> <li>・プリンタ2は正常。</li> <li>・プリンタ3は正常。</li> </ul> <p>【デバイス監視サーバ】</p> <ul style="list-style-type: none"> <li>・プリンタ1は正常。</li> </ul>	<p>【原因】</p> <p>プリンタ1のハードディスクがいっぱいで、スプールデータが正しく格納されていない。</p> <p>【対処】</p> <p>プリンタ1のハードディスクの空き容量を確認する。</p>	
新しくPC2をセットアップしてプリンタ2の設定をしている。プリンタ2は見えないのだが、プリンタ3が見えない。	<p>【PC監視クライアント】</p> <ul style="list-style-type: none"> <li>・プリンタ1は正常。</li> <li>・プリンタ2は正常。</li> <li>・プリンタ3は正常。</li> </ul> <p>【デバイス監視サーバ】</p> <ul style="list-style-type: none"> <li>・プリンタ1は正常。</li> <li>・プリンタ2は正常。</li> <li>・プリンタ3は正常。</li> </ul>	<p>【原因】</p> <p>新規PCは、セグメント越えができていないので、デフォルトゲートウェイが正しく設定されていない。</p> <p>【対処】</p> <p>デフォルトゲートウェイにルータ1のIPアドレスを設定する。</p>	
PC3からプリンタ4にプリントしたが、プリントされない。 昨日まではできていた。	<p>【PC監視クライアント】</p> <ul style="list-style-type: none"> <li>・PC3は正常。</li> </ul> <p>【デバイス監視サーバ】</p> <ul style="list-style-type: none"> <li>・プリンタ4で、ソータの接続不良のアラーム。</li> </ul>	<p>【原因】</p> <p>ソータが正しく接続されていない。</p> <p>【処置】</p> <p>ソータを正しく接続する。</p>	

【図27】



【図 28】

e-Maintenance復旧作業依頼書			
<u>ユーザ情報</u> 顧客名 部署 連絡先(電話) 連絡先(FAX) 連絡先(E-mail)		<u>機器情報</u> 機種 商品企画部 03-3765-XXXX 03-3765-YYYY rds@ZZZZ	
発生時刻 2001年XX月YY日 aa時 bb分		機番/シリアル番号 機種 環境 設置場所 ABC12345 IR5000 1F奥	
<u>コール内容</u> <div style="border: 1px solid black; height: 80px; width: 100%;"></div>			
<u>作業依頼項目</u> <div style="display: flex; justify-content: space-between;"> <span>○ 障害切り分</span> <span>● 復旧作業</span> </div>			
<u>リモートによる障害切り分け内容</u> <div style="border: 1px solid black; height: 80px; width: 100%;"></div>			
<u>対応期限</u> 2001年 XX月 YY日    ZZ時    までに対応をお願いします。			
2001年 XX月 YY日 AAA会社 担当    OO    ΔΔ			

【図 29】

発生時刻	復旧時刻	機種/シリアル番号	現象	原因	処置	担当
2001.3.3 15:35	2001.3.3 14:52	ABC12345	プリントが出力されない。……	部品Aの故障が原因。	部品Aを交換。	〇〇

診断結果

全く問題ありません。快適にお使いいただいています。

障害がありましたが、対処済みなので問題ありません。

故障の頻度が高くなっています。しばらく観察が必要です。

AAA00112, BBB7777, ………
ABC12345
ABC98765

2001年 XX月 YY日      EMセンター  
AAA会社

【図 3 0】

発生時刻	機種/シリアル番号	原因	処置
2001.3.3 15:35	ABC12345	部品Aの故障が原因。	部品Aを交換。

2001年 XX月 YY日  
AAA会社

EMセンター

【書類名】            要約書

【要約】

【課題】    顧客先ののコンピュータと周辺機器とを一元的に管理する遠隔サイト管理システムを提供する。

【解決手段】    遠隔サイト管理システムは、オフィスのサービス対象の機器がエラーを起こし、オフィスの顧客が保守サービス会社に電話で通知（センターコール）したときに、エラー発生に的確に対応し、スムーズにメンテナンスの手配（サービスマンの手配、他のサービス会社への代行メンテナンス依頼）を行なう。

【選択図】            図 2 0

【書類名】 手続補正書  
【提出日】 平成13年 1月11日  
【あて先】 特許庁長官 及川 耕造 殿  
【事件の表示】

【出願番号】 特願2000-351262

【補正をする者】

【識別番号】 000001007

【住所又は居所】 東京都大田区下丸子3丁目30番2号

【氏名又は名称】 キヤノン株式会社

【代表者】 御手洗 富士夫

【電話番号】 03-3758-2111

【代理人】

【識別番号】 100090538

【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会社  
内

【弁理士】

【氏名又は名称】 西山 恵三

【電話番号】 03-3758-2111

【ブルーフの要否】 要

【手続補正 1】

【補正対象書類名】 特許願

【補正対象項目名】 発明者

【補正方法】 変更

【補正の内容】

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キヤノン株式会社  
内

【氏名】 片山 康二郎



【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 中村 真一

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 原 寛行

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 廣瀬 淳一

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 大森 和志

【発明者】

【住所又は居所】 東京都大田区下丸子3丁目30番2号キャノン株式会社  
内

【氏名】 川島 真

【その他】 本件の発明者のうち、原 寛行とすべきところを誤って、  
原 寛之として出願致しましたのでここに訂正を致します。

認定・付加情報

特許出願の番号	特願2000-351262
受付番号	50100028327
書類名	手続補正書
担当官	濱谷 よし子 1614
作成日	平成13年 1月26日

<認定情報・付加情報>

【補正をする者】

【識別番号】

000001007

【住所又は居所】

東京都大田区下丸子3丁目30番2号

【氏名又は名称】

キャノン株式会社

【代理人】

申請人

【識別番号】

100090538

【住所又は居所】

東京都大田区下丸子3丁目30番2号 キャノン  
株式会社内

【氏名又は名称】

西山 恵三

出 願 人 履 歴 情 報

識別番号 [000001007]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都大田区下丸子3丁目30番2号  
氏 名 キヤノン株式会社